IPSec VPN Acceleration Services Module Installation and Configuration Note

Product Number: WS-SVC-IPSEC-1

This publication describes how to install and configure the IPSec Virtual Private Network (VPN) Acceleration Services Module in the Catalyst 6500 series switches and Cisco 7600 Series Internet Routers.

Note Throughout this publication, the IPSec VPN Acceleration Services Module is referred to as the *VPN module*.

Note Throughout this publication, the term *crypto* is used to refer to *cryptographic*.

Note For information on the latest caveats and updates for the VPN module, refer to the following publications:

Cisco IOS Release 12.2(9)YO4 or later release notes at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_2864.htm

Cisco IOS Release 12.2(14)SY or later release notes at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3975.htm

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This publication consists of these sections:

Understanding How the VPN Module Works

These sections describe the functionality of the VPN module:

Overview

The VPN module is a Gigabit Ethernet IPSec cryptographic module that you can install in the Catalyst 6500 series switches and Cisco 7600 Series Internet Routers. The VPN module provides bump-in-the-wire (BITW) IPSec implementation using VLANs.

Note BITW is an IPSec implementation that starts egress packet processing after the IP stack has finished with the packet and completes ingress packet processing before the IP stack receives the packet.

Configuring VPNs using the VPN module is similar to configuring VPNs on routers running Cisco IOS software. When you configure VPNs with the VPN module, you attach crypto maps to VLANs (using interface VLANs); when you configure VPNs on routers running Cisco IOS software, you configure individual interfaces.

Note With the VPN module, crypto maps are still attached to individual interfaces but the set of interfaces allowed is restricted to “interface VLANs.”

When you configure a VPN on the Cisco routers, a packet is sent to a routed interface that is associated with an IP address. If the interface has an attached crypto map, the software checks that the packet is on an access control list (ACL) that is specified by the crypto map. If a match occurs, the packet is transformed (encrypted) before it is routed to the appropriate IPSec peer; otherwise, the packet is routed in the *clear* (unencrypted) state.

When you configure the VPN module, the same cryptographic operations are performed as on Cisco routers. The VPN module's implementation of VPN is generally the same as on Cisco routers other than the use of interface VLANs and some configuration guidelines that are specific to the VPN module (see the "VPN Module Configuration Guidelines" section on page 25 for details).

Note For detailed information on Cisco IOS IPSec cryptographic operations and policies, refer to the "IP Security and Encryption" section of the *Cisco IOS Security Configuration Guide*, Release 12.2.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fipsenc/index.htm

When you configure the VPN module on the Catalyst 6500 series switches and Cisco 7600 Series Internet Routers, you ensure that all packets coming from or going to the Internet pass through the VPN module. The VPN module has an extensive set of policies that validate a packet before the packet is sent onto the local (trusted) LAN. The VPN module can use multiple Fast Ethernet or Gigabit Ethernet ports on other Catalyst 6500 series modules to connect to the Internet through WAN routers. Packets that are received from the WAN routers pass through the VPN module for IPSec processing.

On the local LAN side, traffic between the LAN ports can be routed or bridged on multiple Fast Ethernet or Gigabit Ethernet ports. Because the local LAN traffic is not encrypted or decrypted, it does not pass though the VPN module.

The VPN module does not maintain routing information, route, or change the MAC header of a packet (except for the VLAN ID from one VLAN to another).

Catalyst Switch Outside Ports and Inside Ports

The Fast Ethernet or Gigabit Ethernet ports on the Catalyst 6500 series switch and Cisco 7600 Series Internet Routers that connect to the WAN routers are referred to as *Catalyst switch outside ports*. These ports connect the local LAN to the Internet or to remote sites. Cryptographic policies are applied to the Catalyst switch outside ports.

The Fast Ethernet or Gigabit Ethernet ports on the Catalyst 6500 series switch and Cisco 7600 Series Internet Routers that connect to the local LAN are referred to as *Catalyst switch inside ports*.

The VPN module sends encrypted packets to the Catalyst switch outside ports and decrypted packets to the Policy Feature Card 2 (PFC2) for Layer-3 forwarding to the Catalyst switch inside ports.

VPN Module Outside Port and Inside Port

The VPN module appears to the CLI as a module with two Gigabit Ethernet ports. The VPN module has no external connectors; the Gigabit Ethernet ports connect the VPN module to the switch backplane and Switch Fabric Module (if installed).

One Gigabit Ethernet port handles all the traffic going to and coming from the Catalyst switch outside ports. This port is referred to as the *VPN module outside port*. The other Gigabit Ethernet port handles all traffic going to and coming from the local LAN or inside ports. This port is referred to as the *VPN module inside port*.

Note For detailed information on configuration guidelines and restrictions for the VPN module outside and inside port, see the "VPN Module Configuration Guidelines" section on page 25.

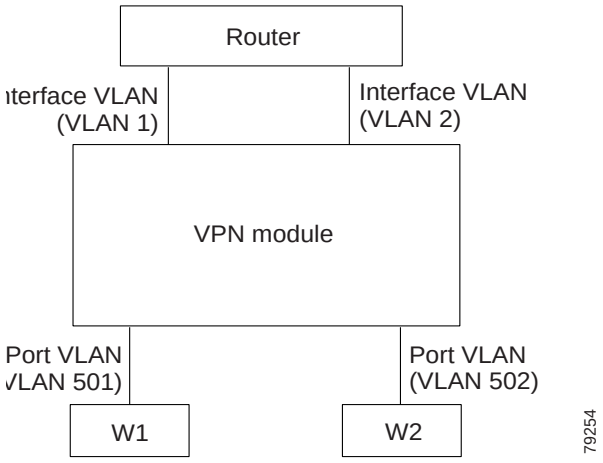
Port VLAN and Interface VLAN

Your VPN configuration can have one or more Catalyst switch outside ports. To handle the packets from multiple Catalyst switch outside ports, you need to direct the packets from multiple Catalyst switch outside ports to the VPN module outside port by placing the Catalyst switch outside ports in a VLAN with the outside port of the VPN module. This VLAN is referred to as the *port VLAN*. The port VLAN is a Layer 2-only VLAN. You do not configure Layer 3 addresses or features on this VLAN; the packets within the port VLAN are bridged by the PFC2.

Before the router can forward the packets using the correct routing table entries, the router needs to know which interface that a packet was received on. For each port VLAN, you need to create another VLAN so that the packets from every Catalyst switch outside port are presented to the router with the corresponding VLAN ID. This VLAN contains only the VPN module inside port and is referred to as the *interface VLAN*. The interface VLAN is a Layer 3-VLAN. You configure the Layer 3 address and Layer 3 features, such as ACLs and the crypto map, to the interface VLAN.

After you create and configure the port VLAN and the interface VLAN, you tie the VLANs together by using a new CLI command (**crypto connect vlan** command). See the "Configuring a VPN Using the VPN Module" section on page 21 for detailed information. Figure 1 shows the port VLAN and interface VLAN configurations.

Figure 1 Port VLAN and Interface VLAN Configuration Example



Port VLAN 501 and port VLAN 502 are the port VLANs that are associated with the Catalyst switch outside ports W1 and W2.

Interface VLAN 1 and interface VLAN 2 are the interface VLANs that correspond to port VLAN 501 and port VLAN 502.

You configure the IP address, ACLs, and crypto map that apply to the Catalyst switch outside port W1 on interface VLAN 1. You configure the features that apply to the Catalyst switch outside port W2 on interface VLAN 2.

Packets coming from the WAN through port W1 (port W1 belongs to port VLAN 501) are directed by the PFC2 to the VPN module outside port. The VPN module decrypts the packets and changes the VLAN to interface VLAN 1 and then presents the packet to the router through the VPN module inside port. The PFC2 then routes the packet to the proper destination.

Packets going from the LAN to the outside ports are first routed by the PFC2. Based on the route, the PFC2 routes the packets to one of the interface VLANs and directs the packet to the VPN module inside port. The VPN module applies the cryptographic policies that are configured on the corresponding interface VLAN, encrypts the packet, changes the VLAN ID to the corresponding port VLAN, and sends the packet to the Catalyst switch outside port through the VPN module outside port.

Supported Features

These sections list the supported features for the VPN module:

- Supported Features in Release 12.2(9)YO4 and Release 12.2(14)SY, page 5
- Supported Features in Release 12.2(14)SY, page 6

Supported Features in Release 12.2(9)YO4 and Release 12.2(14)SY

The VPN module supports the following features in Cisco IOS Release 12.2(9)YO4 and later releases and Cisco IOS Release 12.2(14)SY and later releases:

- IPSec support through Cisco IOS software and the VPN module
  - Certificate Authorities/Public Key Infrastructure (CA/PKI) support
- Tunneling protocols
  - IPSec (IPv4) tunnel and transport modes (RFC 2401)
- IPSec encryption/decryption
  - DES/3DES
  - HMAC-SHA-1
  - HMAC-MD5
- Internet Key Exchange (IKE) acceleration
  - Perfect Forward Secrecy (PFS)
  - RSA encryption
  - RSA signature
  - Diffie-Hellman groups 1, 2, 5
- Interoperability—Interoperable with all Cisco IOS and appliance platforms

- Capacity
  - 8000 tunnels (no IKE keepalive, no Dead-Peer-Detection [DPD])
  - 5000 tunnels (no IKE keepalive, DPD okay)
  - 2000 tunnels (IKE keepalive)

Note DPD is supported in Cisco IOS Release 12.2(14)SY or later releases.

Note Capacities are typically higher when IKE keepalive uses DPD.

- Configuration, management, and reporting
  - Existing Cisco IOS IPSec CLI (one new configuration command, **crypto connect vlan**)
  - Existing standard IPSec network management
- VPN Device Manager (VDM) (requires VPN software release 1.2)

Note VDM contains only basic IPSec support and cannot be used to configure multiple VPN modules or VPN module features added in Cisco IOS Release 12.2(14)SY.

For complete configuration details for VDM, refer to this URL:
http://www.cisco.com//univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e6/vdm_e.htm

Supported Features in Release 12.2(14)SY

The VPN module supports the following features in Cisco IOS Release 12.2(14)SY and later releases:

- Interchassis active/standby IPSec stateful failover
- Easy-VPN clients (the Easy-VPN client version should be 3.6 or later)
- IPSec NAT transparency
- Onboard acceleration of VDM TopN queries for IPSec
- IPSec anti-replay window size expansion from 32 entries to 64 entries
- DPD
- Hot Standby Router Protocol (HSRP) and reverse route injection (RRI)
- Onboard GRE acceleration
- QoS
- Support for up to 10 VPN modules per chassis
- IPSec over the FlexWAN module (WS-X6182-2PA) with the following supported port adapters:
  - PA-4T+: 4-Port serial port adapter, enhanced
  - PA-T3: 1-port T3
  - PA-E3: 1-port E3
  - PA-T3+: 1-port T3 enhanced
  - PA-2T3+: 2-port T3 enhanced

  - PA-MC-2T1: 2-port multichannel T1
  - PA-MC-8T1: 8-port multichannel T1
  - PA-MC-T3: 1-port multichannel T3
  - PA-MC-E3: 1-port multichannel E3
  - PA-A3-T3: T3 ATM
  - PA-A3-OC3MM: OC3 ATM multimode
  - PA-A3-OC3SMI: OC3 ATM single-mode IR
  - PA-A3-OC3SML: OC3 ATM single-mode LR
  - PA-POS-OC3MM: OC3 POS multimode
  - PA-POS-OC3SMI: OC3 POS single-mode IR
  - PA-POS-OC3SML: OC3 POS single-mode LR
  - PA-H: 1-port HSSI
  - PA-2H: 2-port HSSI
- You may have a VPN module in the same chassis with the following service modules:
  - Firewall Services Module (WS-SVC-FWM-1-K9)
  - Intrusion Detection System Module 2 (WS-SVC-IDS2BUNK9)
  - Network Analysis Module 1 (WS-SVC-NAM-1), Network Analysis Module 2 (WS-SVC-NAM-2)

Note You can install a maximum of four service modules of any one kind per chassis (such as four Firewall Services Modules and four Network Analysis Modules per chassis). The exception is the Intrusion Detection System Module 2 (IDSM2); you can only install two IDSM2s per chassis.

Hardware and Software Requirements

This section describes the hardware and software requirements for the VPN module.

Software Requirements

This section lists the software requirements for the VPN module:

- Cisco IOS Release 12.2(9)YO4 or later releases
- Cisco IOS Release 12.2(14)SY or later releases

Hardware Requirements

This section lists the hardware requirements for the VPN module:

- The following Catalyst 6500 series switches are supported:
  - Catalyst 6503 switch
  - Catalyst 6506 switch
  - Catalyst 6509 switch
  - Catalyst 6513 switch

Note With Cisco IOS Release 12.2(9)YO4, you can install only one VPN module per chassis.

Note With Cisco IOS Release 12.2(14)SY or later releases, you can install up to 10 VPN modules per chassis. For more information, see the "Using Multiple VPN Modules in a Chassis" section on page 33.

- The following Cisco 7600 Series Internet Routers are supported:
  - 7603 Internet Router (CISCO7603)
  - 7606 Internet Router (CISCO7606)
  - 7609 Internet Router (CISCO7609)
  - 7609 Internet Router (OSR-7609)

Note The 7606 Internet Router is not supported in Cisco IOS Release 12.2(9)YO4.

- Supervisor Engine 2 (MSFC2 and PFC2)

Note The VPN module MSFC2 DRAM requirements are as follows:

– Up to 500 tunnels with 128-MB DRAM
– Up to 4,000 tunnels with 256-MB DRAM
– Up to 8,000 tunnels with 512-MB DRAM

These numbers are chosen to leave some memory available for routing protocols and other applications. However, your particular use of the MSFC2 may demand more memory than the quantities listed above. In an extreme case, you could have one tunnel but still require 512-MB DRAM for other protocols and applications running on the MSFC2.

For MSFC2 DRAM upgrade information, refer to the following publication at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_6953.htm

- All Catalyst 6500 series Fast Ethernet and Gigabit Ethernet switching modules are supported.

Note The FlexWAN module and the Optical Services Modules (OSMs) are not supported by Cisco IOS Release 12.2(9)YO4.

Support for the FlexWAN module is added with Cisco IOS Release 12.2(14)SY (see the "Supported Features in Release 12.2(14)SY" section on page 6 for a complete list of supported port adapters). OSMs are not supported by Cisco IOS Release 12.2(14)SY.

Front Panel Description

The LED on the VPN module front panel (see Figure 2) indicates the status of the module. Table 1 describes the LED operation.

Figure 2 VPN Module Front Panel

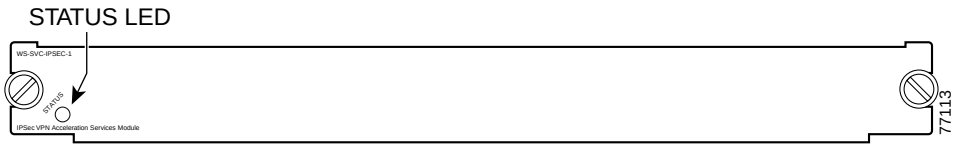


Table 1 VPN Module LED Description

LED	Color/Description
STATUS	The STATUS LED shows the status as follows: • Normal initialization sequence Orange—Module is booting or running diagnostics Green—All diagnostics pass; module is operational • Fault during initialization sequence Orange—Module is booting or running diagnostics Red—Diagnostic test fails; module is not operational • Environmental monitoring Orange—Overtemperature condition (minor threshold exceeded) Red—Overtemperature condition (major threshold exceeded)

Installing and Removing the VPN Module

These sections describe how to remove and install the VPN module in the Catalyst 6500 series switches:

Safety Overview

Safety warnings appear throughout these procedures indicating tasks that may harm you if performed incorrectly. A warning symbol precedes each warning statement.

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.**

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Caution During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

Required Tools

These tools are required to install the VPN module in the Catalyst 6500 series switches:

- Number 2 Phillips-head screwdriver
- Antistatic mat or antistatic foam
- Your own electrostatic discharge (ESD) grounding strap or the disposable ESD strap included with the system

Removing a VPN Module

This section describes how to remove an existing VPN module from a chassis slot.

Caution During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Warning **Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches* publication or the *Regulatory Compliance and Safety Information for the Cisco 7600 Series Internet Routers* publication. These publications contains important safety information you should know before working with the system.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

To remove a VPN module from the chassis, perform these steps:

Step 1 Verify that the captive installation screws on all of the modules in the chassis are tight. This step assures that the space created by the removed module is maintained.

Note If the captive installation screws are loose, the electromagnetic interference (EMI) gaskets on the installed modules will push the modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 2 Loosen the two captive installation screws on the VPN module.

Step 3 Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of the following two sets of steps.

Horizontal slots

a. Place your thumbs on the left and right ejector levers, and simultaneously rotate the levers outward to unseat the module from the backplane connector.

b. Grasp the front edge of the module, and slide the module part of the way out of the slot. Place your other hand under the module to support the weight of the module. Do not touch the module circuitry.

Vertical slots

a. Place your thumbs on the ejector levers that are located at the top and bottom of the module, and simultaneously rotate the levers outward to unseat the module from the backplane connector.

b. Grasp the edges of the module, and slide the module straight out of the slot. Do not touch the module circuitry.

Step 4 Place the module on an antistatic mat or antistatic foam, or immediately reinstall it in another slot.

Step 5 If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the chassis.

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.**

Installing a VPN Module

This section describes how to install a VPN module in the chassis.

Caution To prevent ESD damage, handle modules by the carrier edges only.

Caution During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Warning **Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches* publication or the *Regulatory Compliance and Safety Information for the Cisco 7600 Series Internet Routers* publication. These publications contains important safety information you should know before working with the system.**

To install a VPN module in the chassis, perform these steps:

Step 1 Choose a slot for the VPN module.

Step 2 If possible, place VPN modules between empty slots that contain only module filler plates.

Step 3 Verify that the captive installation screws are tightened on all modules that are installed in the chassis. This step assures that the EMI gaskets on all modules are fully compressed in order to maximize the opening space for the new module or the replacement module.

Note If the captive installation screws are loose, the EMI gaskets on the installed modules will push adjacent modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 4 Remove the module filler plate by removing the two Phillips pan-head screws from the filler plate. To remove a module, see the "Removing a VPN Module" section on page 12.

Step 5 Fully open both ejector levers on the new or replacement module. (See Figure 3.)

Step 6 Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of the two following sets of substeps.

Horizontal slots

a. Position the VPN module in the slot. (See Figure 3.) Make sure that you align the sides of the module carrier with the slot guides on each side of the slot.

b. Carefully slide the VPN module into the slot until the EMI gasket along the top edge of the module makes contact with the module in the slot above it and both ejector levers have closed to approximately 45 degrees with respect to the module faceplate. (See Figure 4.)

c. Using the thumb and forefinger of each hand, grasp the two ejector levers and press down to create a small (0.040 inch [1 mm]) gap between the module's EMI gasket and the module above it. (See Figure 4.)

Caution Do not exert too much pressure on the ejector levers because you will bend and damage them.

Vertical slots

a. Position the VPN module in the slot. (See Figure 6.) Make sure that you align the sides of the switching-module carrier with the slot guides on the top and bottom of the slot.

b. Carefully slide the VPN module into the slot until the EMI gasket along the right edge of the module makes contact with the module in the slot adjacent to it and both ejector levers have closed to approximately 45 degrees with respect to the module faceplate. (See Figure 7.)

c. Using the thumb and forefinger of each hand, grasp the two ejector levers and exert a slight pressure to the left, deflecting the module approximately 0.040 inches (1 mm) to create a small gap between the module's EMI gasket and the module adjacent to it. (See Figure 7.)

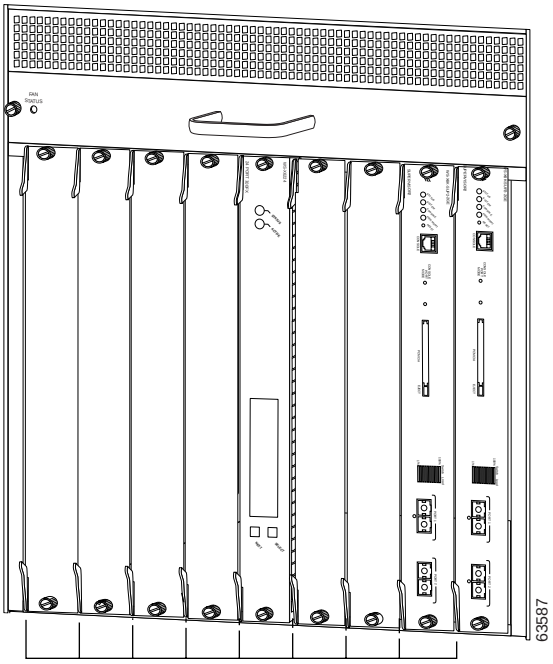
Caution Do not exert too much pressure on the ejector levers because you will bend and damage them.

d. While pressing on the ejector levers, simultaneously close them to fully seat the VPN module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate. (See Figure 8.)

e. Tighten the two captive installation screws on the module.

Note Make sure that the ejector levers are fully closed before tightening the captive installation screws.

Figure 8 Ejector Lever Closure in a Vertical Slot Chassis



Verifying the Installation

Enter the **show module** [*mod-num* | **all**] command to verify that the system acknowledges the new VPN module and has brought it online.

This example shows the output of the **show module** command:

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1     2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2   SAD055106AH
  2    16  SFM-capable 16 port 1000mb GBIC        WS-X6516-GBIC      SAD0546024C
  4    48  SFM-capable 48-port 10/100 Mbps RJ45   WS-X6548-RJ-45     SAD060904PU
  5     2  IPSec VPN Accelerator                  WS-SVC-IPSEC-1     SAD0636025E

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  0002.7e38.6c4c to 0002.7e38.6c4d   3.2   6.1(3)       6.2(2.107)   Ok
  2  0002.7ee0.28c0 to 0002.7ee0.28cf   3.0   6.1(3)       6.2(2.107)   Ok
  4  0001.63d6.94da to 0001.63d6.9509   4.2   6.3(1)       6.2(2.107)   Ok
  5  0060.0217.0000 to 0060.0217.0000   1.0   7.2(0.74-Eng 6.2(2.107)   Ok

Mod Sub-Module                  Model           Serial          Hw     Status
--- --------------------------- --------------- --------------- ------- -------
  1 Policy Feature Card 2       WS-F6K-PFC2     SAD055200K7     3.0    Ok
  1 Cat6k MSFC 2 daughterboard  WS-F6K-MSFC2    SAD055107JD     2.0    Ok
Router#
```

Configuring a VPN Using the VPN Module

These sections describe how to configure a VPN using the VPN module:

Tip To ensure a successful configuration of your VPN using the VPN module, read all of the configuration summaries and guidelines before you perform any configuration tasks.

Hardware- and Software-Based Cryptographic Modes

When the VPN module is configured and active in the chassis, software encryption by the MSFC2 is disabled. This mode of operation is referred to as hardware-based cryptographic mode. In hardware-based cryptographic mode, any software-based cryptographic configurations that use the MSFC2 have an undefined or unspecified effect. In hardware-based cryptographic mode, if you associate a crypto ACL with a non-VLAN interface, packets do not get encrypted or dropped. You need to remove the software-based cryptographic configuration from the interface and then configure the interface correctly for hardware-based cryptographic operation with the VPN module.

Transitioning In and Out of Hardware-Based Cryptographic Mode

When you add the **crypto connect vlan** command to the running configuration, you enter hardware-based cryptographic mode. When you remove the last **crypto connect vlan** command from the running configuration (using the **no crypto connect vlan** command), you exit the hardware-based cryptographic mode.

Note Switching to the software-based cryptographic mode (by entering the **no crypto connect vlan** command) does not automatically change the configuration and enable software-based cryptographic operation. To enable software-based cryptographic mode and have it function correctly, you have to remove the VPN module configuration and reconfigure the switch for software-based cryptographic operation.

Effects of Exiting the Hardware-Based Cryptographic Mode on Existing IPSec SAs

These sections describe the configuration guidelines for exiting the hardware-based cryptographic mode on existing IPSec SAs.

Cisco IOS Release 12.2(9)YO4 or Later Releases

The configuration guidelines for Cisco IOS Release 12.2(9)YO4 or later releases are as follows:

- When you enter the **no crypto connect vlan** command to break the connection between a port VLAN and the interface VLAN, the IPSec security associations (SAs) are not automatically removed.

  Note The IPSec SAs may be removed by other features such as DPD or IKE keepalives.

- If the **no crypto connect vlan** command is the *last* hardware-based cryptographic configuration command that you entered, then the IPSec SAs are removed automatically as part of the switchover from hardware-based cryptographic mode to software-based cryptographic mode.

Cisco IOS Release 12.2(14)SY and Later Releases

The configuration guidelines for Cisco IOS Release 12.2(14)SY or later releases are as follows:

- When you issue the **no crypto connect vlan** command on a crypto-connected routed, access, or trunk mode port, all the associated SAs are removed.
- When you shut down a port VLAN, none of the associated SAs are removed.
- When you shut down an interface VLAN, the hardware-based cryptographic mode will not be exited.
- When you shut down an interface VLAN, all the associated SAs will not be removed.
- When you enter the **no ip address** command on an interface VLAN, all the associated SAs will not be removed.
- When you change the IP address on an interface VLAN by entering the **ip address** *new-ip-address new-mask* command, all the associated SAs are removed.

Note that the behavior described above depends on the type of interface as follows:

- Ethernet interface:
  - shut down—SAs are removed.
  - no shut down—SAs are recreated on the VPN module.

- WAN interface:
  - shut down (on reload)—No SAs are created on the VPN module (must do a no shut down first).
  - no shut down (first no shut down issued after a reload)—SAs are created on the VPN module.
  - shut down (after a no shut down)—SAs remain active on the VPN module.
- Access/trunk mode ports:
  - shut down—SAs are never removed.

Configuration Summaries

These sections provide Ethernet configuration summaries for the three modes of operation that are supported by the VPN module:

Note For WAN interface configuration, see the "Using WAN Interfaces" section on page 45.

Access Port Mode Summary

This section summarizes the steps that are required to configure a Catalyst switch outside port as an access port (see the "Configuring a VPN Access Port Connection" section on page 52 for detailed information):

1. Perform the following standard Cisco IOS encryption tasks:
   a. Create an IKE policy, if necessary.
   b. Create a preshared key entry, if necessary.
   c. Create an ACL.
   d. Create a crypto map.
2. Add an inside interface VLAN and outside access port VLAN to the VLAN database.
3. Create a Layer 3 inside interface VLAN, and attach a crypto map.
4. Create an outside interface VLAN for the outside access port VLAN.
5. Add the inside interface VLAN as an allowed VLAN to the VPN module inside trunk port (the VPN module ports are trunk ports by default).
6. Add a Catalyst switch outside port to the outside access port VLAN, and connect the outside access port VLAN to the inside interface VLAN using the **crypto connect vlan** command.

Note You can do the crypto connection from the port or from the port VLAN interface, but the **crypto connect vlan** command will always appear in the configuration of the port VLAN.

Routed Port Mode Summary

This section summarizes the steps that are required to configure a Catalyst switch outside port as a routed port (see the "Configuring a VPN Routed Port Connection" section on page 54 for detailed information):

1. Perform the following standard Cisco IOS encryption tasks:
   a. Create an IKE policy, if necessary.
   b. Create a preshared key entry, if necessary.
   c. Create an ACL.
   d. Create a crypto map.
2. Add an inside interface VLAN to the VLAN database.
3. Create a Layer 3 inside interface VLAN, and attach a crypto map.
4. Add the inside interface VLAN as an allowed VLAN to the VPN module inside trunk port (the VPN module ports are trunk ports by default).
5. Connect the outside Catalyst routed port to the inside interface VLAN using the **crypto connect vlan** command.

Trunk Port Mode Summary

Caution When you configure an Ethernet port as a trunk port, all the VLANs are allowed on the trunk port by default. This default configuration does not work well with the VPN module and causes network loops. For detailed information on configuring trunks, see the "Trunks" section in the "Interaction with Other Features" section on page 25.

This section summarizes the steps that are required to configure a Catalyst switch outside port as a trunk port (see the "Configuring a VPN Trunk Port Connection" section on page 55 for detailed information):

1. Perform the following standard Cisco IOS encryption tasks:
   a. Create an IKE policy, if necessary.
   b. Create a preshared key entry, if necessary.
   c. Create an ACL.
   d. Create a crypto map.
2. Add an inside interface VLAN and outside trunk port VLAN to the VLAN database.
3. Create a Layer 3 inside interface VLAN, and attach a crypto map.
4. Add the inside interface VLAN as an allowed VLAN to the VPN module inside trunk port (the VPN module ports are trunk ports by default).
5. Create the outside trunk port VLAN interface, and connect it to the inside interface VLAN using the **crypto connect vlan** command.
6. Configure a Catalyst switch outside port as a trunk port, and add the outside trunk port VLAN as an allowed VLAN to the outside port trunk.

VPN Module Configuration Guidelines

Use the guidelines in the following sections when configuring a VPN using the VPN module:

Interaction with Other Features

Follow these configuration guidelines for configuring a VPN using the VPN module:

- EtherChannels

  You can enter the **crypto connect vlan** command only from the following:

  – The associated port VLAN interface when the EtherChannel interface (port-channel interface) and participating interfaces are switch ports

  – The EtherChannel interface when the EtherChannel interface (port-channel interface) and participant interfaces are routed ports

- ACL on a routed port without an IP address

  When a routed port has a crypto connection, the IP ACLs that are attached to the routed port work correctly even if the routed port does not have an IP address.

- HSRP configuration

  – Do not use the **standby use-bia** command. Always use a virtual HSRP MAC address for the router's MAC address.

  – HSRP/GRE is supported.

Note For an example, see the "HSRP" section on page 88.

- Switched Port Analyzer (SPAN)

  Interaction with the SPAN feature is as follows:

  – If the SPAN session is set up to copy all the traffic from the VPN module inside port, then all the traffic before encryption and after decryption is sent to the SPAN port.

  – If the SPAN session is set up to copy all the traffic from the VPN module outside port, then all the traffic before decryption and after encryption is sent to the SPAN port.

  – If the SPAN session is set up to copy all the traffic from the Catalyst switch outside port (the port that connects to the WAN router), then all the traffic before decryption and after encryption is sent to the SPAN port.

- GRE tunnel interfaces

  Attaching a crypto map set to a generic routing encapsulation (GRE) tunnel interface is not supported. You can attach a crypto map set to a GRE tunnel interface, but there are configuration restrictions. You can configure the GRE tunnel interface in the same manner as on other Cisco routers, but you cannot attach a crypto map set to the interface. Instead, you attach the crypto map set to all of the ingress/egress interfaces over which the GRE tunnel spans. Note that HSRP/GRE is supported.

Note For detailed configuration information, see the "Using GRE Tunneling" section on page 49.

Preventing VPN Module Misconfigurations

Follow these guidelines to prevent VPN module misconfigurations:

- Removing a line in a crypto ACL causes all crypto maps using that ACL to be removed and reattached to the VPN module. This action causes all the SAs that are derived from the crypto maps, which referenced that ACL, to flap.
- Do not convert existing crypto-connected port characteristics. When the characteristics of a crypto-connected access port or a routed port change (switch port to routed port or vice versa), the associated crypto connection is deleted.
- The example in this section shows how a misconfiguration can affect the startup-configuration file. This example uses the following configuration:

  – The interface VLAN is 100.

  – The port VLAN is 200 on access port Gigabit Ethernet 1/1.

  – The VPN module is in slot 2.

  In this example, a crypto connection exists, and when the associated interface VLAN is removed from the VPN module inside port, a misconfigured startup-configuration file is created.

Note With Cisco IOS Release 12.2(14)SY, it is no longer possible to remove an interface VLAN from the VPN module inside port while the crypto connection to the interface VLAN exists. You must first remove the crypto connection.

When you enter the **write memory** command, the following misconfigured startup-configuration file is created:

```
.
.
.
interface GigabitEthernet1/1
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 200
 switchport mode access
 crypto connect vlan 100
end
.
.
.
interface GigabitEthernet2/1
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005 <-- misconfiguration
 switchport mode trunk
 flowcontrol receive on
 cdp enable
end
.
.
.
```

In this example, when you use this startup-configuration file to boot a switch, the misconfigured crypto connections are removed after the VPN module boots and this warning message is displayed:

```
%CRYPTO: crypto connection to VLAN 100 is removed from gi1/1 because VLAN 100 doesn't
belong to any IPSec Service Module.
```

Note that all the configurations on the interface VLAN, such as the crypto map, are intact.

- Do not remove the interface VLAN or port VLAN from the VLAN database. All interface VLANs and port VLANs must be in the VLAN database. When you remove these VLANs from the VLAN database, the running traffic stops.

  When you enter the **crypto connect vlan** command and the interface VLAN or port VLAN is not in the VLAN database, this warning message is displayed:

  ```
  VLAN id 100 not found in current VLAN database. It may not function correctly unless
  VLAN 100 is added to VLAN database.
  ```

- When replacing a crypto map on an interface, always enter the **no crypto map** *name* [**redundancy** | **ssp** *group*] command before reapplying a crypto map on the interface.

Miscellaneous Guidelines

Follow these configuration guidelines for configuring a VPN using the VPN module:

- Loopback interfaces

  Attaching a crypto map set to a loopback interface is not supported. However, you can maintain an IPSec security association database independent of physical ingress/egress interfaces with the VPN module by entering the **crypto map** *map-name* **local-address** *interface* command.

  If you apply the same crypto map set to each secure interface and enter the **crypto map** *map-name* **local-address** *interface* command with *interface* as a loopback interface, you will have a single security association database for the set of secure interfaces.

- **show crypto vlan** command

  When the interface VLAN belongs to the VPN module inside port, the **show crypto vlan** command output is as follows:

  ```
  Interface VLAN 2 on IPSec Service Module port 7/1 connected to Fa8/3
  ```

  When there is a crypto connection, but the VPN module inside port does not include the interface VLAN due to a misconfiguration, the output is as follows:

  ```
  Interface VLAN 2 connected to Fa8/3 (no IPSec Service Module attached)
  ```

  Note With Cisco IOS Release 12.2(14)SY, it is no longer possible to remove an interface VLAN from the VPN module inside port while the crypto connection to the interface VLAN exists. You must first remove the crypto connection.

- **show crypto engine configuration** command

  The **show crypto engine configuration** command does not show the VPN module slot number when there is no crypto connection even if the module is installed in the chassis.

- Supervisor engine switchover

  After a supervisor engine switchover, the installed modules reboot and come back online. During this period, the VPN module's established tunnels (SAs) are temporarily lost and are reconstructed after the VPN module comes back online. The reconstruction is through IKE (it is not instantaneous).

- Switching module removal

  When you remove a switching module that has some ports participating in crypto connection, the crypto connections remain intact. When you reinsert the same type of switching module, the traffic starts to run again on all the crypto connections. You must manually remove the crypto connections that are associated with the removed switching module. You can enter the **no crypto connect vlan** command from any interface when the associated physical port is removed.

- Rebooting a VPN module with crypto connections

  When you reboot a VPN module that has crypto connections, the existing crypto connections are kept intact. The traffic starts running again when the VPN module reboots. When a crypto connection exists but the associated interface VLAN is missing from the VPN module inside port, the crypto connection is removed after the VPN module reboots.

- When you remove a port VLAN or an interface VLAN with the **no interface vlan** command, the associated crypto connection is also removed.

- With Cisco 7200 Series Routers and other Cisco software crypto platforms, if you configure a crypto map with an empty ACL (an ACL that is defined but has no lines) and attach the crypto map to an interface, all traffic going out of that interface is dropped. However, with the VPN module, all traffic goes out of the interface in the clear (unencrypted) state.

Handling Multicast Traffic

In Cisco IOS Release 12.2(9)YO and later releases, when a chassis contains a Switch Fabric Module the VPN module drops all multicast traffic. This action does not occur if there is no Switch Fabric Module installed. To handle this multicast traffic issue, in Cisco IOS Release 12.2(14)SY and later releases, the Cisco IOS software recognizes when a VPN module has been inserted into a chassis where there is a Switch Fabric Module and automatically configures a SPAN session to forward the multicast traffic.

Note The Firewall Services Module (WS-SVC-FWM-1-K9) and the Multiprocessor WAN Application Module (WS-SVC-MWAM-1) have the same multicast traffic issues as the VPN module. Although this publication covers the VPN module only, note that the other two service modules behave exactly as the VPN module when handling multicast traffic.

See Table 2 for the descriptions of the switching modes that are used when the Switch Fabric Module is installed.

Table 2 Switching Modes with Switch Fabric Module Installed

Modules	Switching Modes
Between fabric-enabled modules (no nonfabric-enabled modules installed)	Compact
Between fabric-enabled modules (when nonfabric-enabled modules are also installed)	Truncated
Between fabric-enabled and nonfabric-enabled modules	Flow-through
Between non-fabric-enabled modules	Flow-through

Follow these guidelines for multicast traffic:

- With a Supervisor Engine 2, if there are two local SPAN sessions or one Remote SPAN (RSPAN) source session configured, the Cisco IOS software cannot generate another session for the VPN module multicast traffic. With this configuration, when you insert a VPN module, a syslog message is displayed directing you to remove one SPAN session.
- When you insert a VPN module and the system is in compact mode, one SPAN session is used (if available). If the system is in flow-through mode or truncated mode, the VPN module uses flow-through mode.
- If you install multiple service modules with the multicast traffic issue, they use the same SPAN session for forwarding multicast traffic. Use the **show monitor** command to display the current SPAN configuration.
- If you insert a VPN module in a chassis that is in compact mode and the two local SPAN sessions or one Remote SPAN (RSPAN) source session are already configured, the switch is put in compact mode. In this situation, all multicast traffic that is sourced from the VPN module is dropped. A syslog message is displayed directing you to remove one SPAN session.
- With a VPN module installed, if you insert a Switch Fabric Module in a chassis that is in flow-through mode and the two local SPAN sessions or one Remote SPAN (RSPAN) source session are already configured, the switch is put in compact mode. In this situation, all multicast traffic that is sourced from the VPN module is dropped. A syslog message is displayed directing you to remove one SPAN session.

- If you insert a VPN module in a chassis that is in compact mode and the VPN module uses one of the automatically configured SPAN sessions without any problems, the system allows you to remove the VPN module and then manually configure both SPAN sessions. However, if you reinsert the VPN module, it is put in compact mode. In this situation, all multicast traffic that is sourced from the VPN module is dropped. A syslog message is displayed directing you to remove one SPAN session.
- When you remove the last service module with the multicast issue from a chassis, the automatically configured SPAN session is cleared and made available for other use. The automatically configured SPAN session is also cleared when the last installed service module changes state from compact to flow-through mode.
- If you do not want to use the automatically configured SPAN session, you can clear the session using the **no monitor session** *session_no* command.
- If you have cleared the automatically configured SPAN session and then want to reconfigure it without OIRing the VPN module, use the **monitor session 1 service-module** command.

Configuring MTU Settings

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

There are two MTU settings on the switch:

- Global—The global MTU setting is used for dropping received packets whose length is greater than the specified MTU value. The global MTU value applies to all chassis ports. You use the **system jumbomtu** command in the global configuration mode to specify the global MTU.
- Interface—The interface MTU setting is used for fragmenting packets. You use the **mtu** command in the interface configuration mode to specify the interface MTU.

Configurable interface MTU values depend on the interface type as follows:

- The Fast Ethernet interface MTU is 1500 bytes (fixed, not configurable)
- The Gigabit Ethernet interface MTU is as follows:
  - On a switch port, 1500 bytes is the default (use the **no mtu** command) or 9216 bytes (use the **mtu 9216** command)
  - On a routed port, use any value from 1500 bytes to 9216 bytes (use the **mtu** *1500-9216* command)
  - On a Gigabit Ethernet interface, each Gigabit Ethernet interface can have a different interface MTU value.
- The MTU for WAN interfaces is a variety of values depending on the encapsulation used.
- The MTU for the VPN module interfaces is 4500 bytes (fixed, not configurable)

The switch makes forwarding decisions that are based on the MTU settings as follows:

- The interface MTU setting is 1500 bytes. If the received packet length is greater than 1500 bytes, the packets are dropped.

- The interface MTU setting is greater than 1500 bytes:
  - If the received packet length is greater than the global MTU value, the packets are dropped.
  - If the received packet length is less than or equal to the global MTU value, routing is performed and the outgoing interface is determined as the result of routing. Then, one of the following conditions apply:

    If the received packet length is greater than the outgoing interface's interface MTU value, the packets are sent to the MSFC2 to be fragmented.

    If the received packet length is less than or equal to the outgoing interface's interface MTU value, the packets are sent directly to the outgoing interface through hardware (PFC2).

Configuring Trunk Ports

Caution When you configure an Ethernet port as a trunk port, all the VLANs are allowed on the trunk port by default. This default configuration does not work well with the VPN module and causes network loops.

When you configure a trunk port for cryptographic connection, do not use the "all VLANs allowed" default. You need to explicitly specify all the desirable VLANs using the **switchport trunk allowed vlan** *vlan-list* command.

To verify the VLANs allowed by a trunk port, enter the **show interface trunk** command or the **show int** *interface* **trunk** command. The following display shows that all VLANs are allowed:

```
cat6k# show interfaces GigabitEthernet 2/1 trunk

Port      Mode         Encapsulation  Status        Native vlan
Gi2/1     on           802.1q         trunking      1

Port      Vlans allowed on trunk
Gi2/1     1-4094

Port      Vlans allowed and active in management domain
Gi2/1     1-4,7-8,513,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Gi2/1     1-4,7-8,513,1002-1005
cat6k#
```

Due to an incorrect startup configuration or through the default trunk port configuration, an interface VLAN might be associated with a trunk port. When you try to remove the interface VLAN from the VLAN list, you might receive an error message similar to the following:

Router# **conf t**

Router(config)# **int g1/1**

Router(config-if)# **switchport trunk allowed vlan rem 71**

```
Command rejected:VLAN 61 is crypto connected to Vl62.
```

To remove the interface VLAN from the VLAN list, enter the following commands:

Router# **conf t**

Router(config)# **int g1/1**

Router(config-if)# **no switchport mode trunk**

Router(config-if)# **switchport trunk allowed vlan 1**

Router(config-if)# **switchport mode trunk**

Router(config-if)# **switchport trunk allowed vlan add** *vlan-list*

Note VLANs in the *vlan-list* must not include any interface VLANs.

To avoid getting into the above situation, when you put an Ethernet port into the trunk mode, enter the following commands in the exact order given:

Router# **conf t**

Router(config)# **int g1/1**

Router(config)# **no shut**

Router(config-if)# **switchport**

Router(config-if)# **switchport trunk allowed vlan 1**

Router(config-if)# **switchport trunk encapsulation dot1q**

Router(config-if)# **switchport mode trunk**

Router(config-if)# **switchport trunk allowed vlan add** *vlan-list*

Note VLANs in the *vlan-list* must not include any interface VLANs.

A common mistake when configuring a trunk port occurs when you use the **add** option as follows: **switchport trunk allowed vlan add 100.** If the **switchport trunk allowed vlan** *vlan-list* command has not already been used, the **add** option *does not* make VLAN 100 the only allowed VLAN on the trunk port; all VLANs are still allowed after entering the command because all the VLANs are allowed by default. After you use the **switchport trunk allowed vlan** *vlan-list* command to add a VLAN, you can then use the **switchport trunk allowed vlan add** *vlan-list* command to add additional VLANs.

Note To remove unwanted VLANs from a trunk port, use the **switch trunk allowed vlan remove** command

Caution Do not enter the **switchport trunk allowed vlan all** command on a secured trunk port. In addition, do not set the VPN module inside and outside ports to “all VLANs allowed.”

Configuring the VPN Module Inside Port and Outside Port

Follow these guidelines for configuring the VPN module inside port and outside port:

- Do not configure the VPN module outside port. Cisco IOS software configures the port automatically.
- Do not change the port characteristics of the VPN module inside port. If you accidentally change the port characteristics, enter the following commands to return the port characteristics to the defaults:

```
Router(config-if)# switchport
Router(config-if)# no switchport access vlan
Router(config-if)# switchport trunk allowed vlan 1,1002-1005
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
```

- Do not remove a VLAN from the VPN module inside port. The running traffic stops when you remove an interface VLAN from the VPN module inside port while the crypto connection to the interface VLAN exists. The crypto connection is not removed and the **crypto connect vlan** command still shows up in the **show running-config** command display. If you enter the **write memory** command with this running configuration, your startup-configuration file would be misconfigured.

Note With Cisco IOS Release 12.2(14)SY, it is no longer possible to remove an interface VLAN from the VPN module inside port while the crypto connection to the interface VLAN exists. You must first remove the crypto connection.

- Do not remove a VLAN from the VPN module outside port. The running traffic stops when you remove a port VLAN from the VPN module outside port while the crypto connection to the interface VLAN exists. The crypto connection is not removed and the **crypto connect vlan** command still shows up in the **show running-config** command display. Removing a VLAN from the VPN module outside port does not affect anything in the startup-configuration file because the port VLAN is automatically added to the VPN module outside port when the **crypto connect vlan** command is entered.

Using Multiple VPN Modules in a Chassis

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

Follow these guidelines when configuring multiple VPN modules in a chassis:

- You can deploy up to ten VPN modules in a single chassis, with the restriction that no more than one VPN module may be used to perform IPSec services for any given interface VLAN.
- Note that using the **no switchport** command followed by the **switchport** command re-adds all VLANs to a trunk port (this situation occurs when you are first switching to a routed port and then back to a switch port). For detailed information on configuring trunks, see the “Trunks” section in the “Interaction with Other Features” section on page 25.

- As with single VPN module deployments, you must properly configure each VPN module's inside and outside port. You can add an interface VLAN only to the inside port *of one* VPN module. Do not add the same interface VLAN to the inside port of more than one VPN module.

  Assigning interface VLANs to the inside ports of the VPN modules allow you to decide which VPN module can be used to provide IPSec services for a particular interface VLAN.

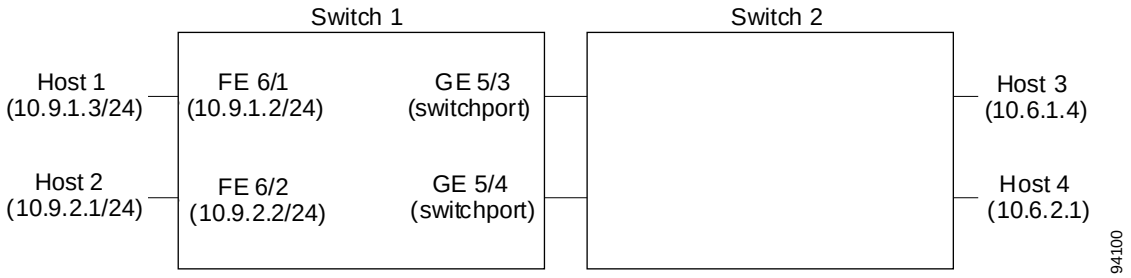
Note There is no support for using more than one VPN module to do IPSec processing for a single interface VLAN.

- SA-based load balancing is not supported.
- The crypto map local address command does not cause SA databases to be shared among multiple VPN modules.

A summary of the switch 1 configuration that is used in the configuration example is as follows (see Figure 9).

- A VPN module is in slot 2 and slot 3 of switch 1.
- In the configuration example, three exclamation points (!!!) precede descriptive comments.

Figure 9 Configuring Multiple VPN Modules Example



The following is a configuration example for switch 1:

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key mykey address 10.8.1.1
crypto isakmp key mykey address 10.13.1.1
!
crypto ipsec transform-set xform1 ah-md5-hmac esp-des esp-sha-hmac
crypto ipsec transform-set xform2 esp-3des esp-sha-hmac
!
!!! crypto map applied to VLAN 12, which is
!!! assigned to "inside" port of VPN-SM in slot 3
crypto map cmap2 10 ipsec-isakmp
 set peer 10.8.1.1
 set transform-set xform1
 match address 102
!
!!! crypto map applied to VLAN 20, which is
!!! assigned to "inside" port of VPN-SM in slot 2
crypto map cmap3 10 ipsec-isakmp
 set peer 10.13.1.1
```

```
 set transform-set xform2
 match address 103
!
!!! "inside" port of VPN-SM in slot 2:
!!! encrypts traffic from VLAN 20, sending encrypted
!!! packets to VLAN 19 via "outside" port Gig2/2
interface GigabitEthernet2/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,20,1002-1005
 switchport mode trunk
 cdp enable
!
!!! "outside" port of VPN-SM in slot 2:
!!! decrypts traffic from VLAN 19, sending decrypted
!!! packets to VLAN 20 via "inside" port Gig2/1
interface GigabitEthernet2/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,19,1002-1005
 switchport mode trunk
 cdp enable
!
!!! "inside" port of VPN-SM in slot 3:
!!! encrypts traffic from VLAN 12, sending encrypted
!!! packets to VLAN 11 via "outside" port Gig3/2
interface GigabitEthernet3/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,12,1002-1005
 switchport mode trunk
 cdp enable
!
!!! "outside" port of VPN-SM in slot 3:
!!! decrypts traffic from VLAN 11, sending decrypted
!!! packets to VLAN 12 via "inside" port Gig3/1
interface GigabitEthernet3/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,11,1002-1005
 switchport mode trunk
 cdp enable
!
!!! "port" VLAN, crypto connected to VLAN 12 by VPN-SM on slot 3
interface Vlan11
 no ip address
 crypto connect vlan 12
!
!!! "interface" VLAN, assigned to VPN-SM on slot 3
interface Vlan12
 ip address 10.8.1.2 255.255.0.0
 crypto map cmap2
!
!!! "port" VLAN, crypto connected to VLAN 20 by VPN-SM on slot 2
interface Vlan19
 no ip address
```

```
 crypto connect vlan 20
!
!!! "interface" VLAN, assigned to VPN-SM on slot 2
interface Vlan20
 ip address 10.13.1.2 255.255.0.0
 crypto map cmap3
!
!!! connected to Host 1
interface FastEthernet6/1
 ip address 10.9.1.2 255.255.255.0
!
!!! connected to Host 2
interface FastEthernet6/2
 ip address 10.9.2.2 255.255.255.0
!
!!! connected to Switch 2
interface GigabitEthernet5/3
 switchport
 switchport mode access
 switchport access vlan 11
!
!!! connected to Switch 2
interface GigabitEthernet5/4
 switchport
 switchport mode access
 switchport access vlan 19
!
ip classless
!
!!! packets from Host 1 to Host 3 are routed from FastEthernet6/1
!!! to VLAN 12, encrypted with crypto map cmap2
!!! using VPN-SM in slot 3, and forwarded to peer 10.8.1.1
!!! through GigabitEthernet5/3
ip route 10.6.1.4 255.255.255.255 10.8.1.1
!
!!! packets from Host 2 to Host 4 are routed from FastEthernet6/2
!!! to VLAN 20, encrypted with crypto map cmap3
!!! using VPN-SM in slot 2, and forwarded to peer 10.13.1.1
!!! through GigabitEthernet5/4
ip route 10.6.2.1 255.255.255.255 10.13.1.1
!
!!! ACL matching traffic between Host 1 and Host 3
access-list 102 permit ip host 10.9.1.3 host 10.6.1.4
!
!!! ACL matching traffic between Host 2 and Host 4
access-list 103 permit ip host 10.9.2.1 host 10.6.2.1
```

Using IPSec Stateful Failover and the VPN Module

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

For complete configuration information for Cisco IOS IPSec stateful failover support, refer to this URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a0080116d4c.html

Follow these guidelines when configuring IPSec stateful failover:

- When configuring an IPSec stateful failover with the VPN module, note that all VPN module configuration rules apply. You must apply crypto maps to interface VLANs, and you must attach interface VLANs to the VPN module inside port.
- When configuring an IPSec stateful failover with a VPN module in two chassis, note that the hardware configurations of both chassis must be exactly the same. For example, in one chassis if the VPN module that is in slot 2 is used to protect interface VLAN 100 and the VPN module that is in slot 3 is used to protect interface VLAN 101, the exact same configuration must be reflected in the second chassis. An example of a misconfiguration would be if the VPN module in slot 3 of the second chassis is used to protect interface VLAN 100.
- Do not use an IPSec stateful failover with Easy-VPN clients or IKE keepalives. An IPSec stateful failover may be used with peers when DPD is used.
- Do not add nonexistent or inadequately configured HSRP standby groups to the state synchronization protocol (SSP) configuration because this action disables high-availability features until the configuration is corrected.
- The recommended HSRP timer values are 1 second for hello timers and 3 seconds for hold timers. These values should prevent an undesirable failover that is caused by temporary network congestion or transient, high CPU loads.

  These timer values can be adjusted upward if you are running high loads or have a large number of HSRP groups. Temporary failures and load-related system stability can be positively affected by raising the timer values as needed. The hello timer value should be approximately a third of the hold timer value.
- Use the HSRP “delay” timers to allow a device to finish booting/initializing/synchronizing before participating as a high-availability pair. Set the “minimum” delay at 30 seconds or more to help prevent active/standby flapping and set the “reload” delay at some value greater than the minimum. You can use the delay timers to reflect the complexity and size of a particular configuration on various hardware. The delay timers tend to vary from platform to platform.
- Sequence number updates from active to standby have a 20-second minimum interval per SA.
- Due to dependence on HSRP, an IPSec stateful failover does not work for secured WAN ports (IPSec over FlexWAN module port adapters).
- Use the reverse route injection (RRI) feature to allow dynamic routing information updates during the HSRP and IPSec failover. For complete configuration information on RRI support, refer to this URL:
  http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_tech_note09186a00800942f7.shtml

The following is a configuration example for the active chassis that is configured for an IPSec stateful failover (at the end of this example, see the configuration example for the standby chassis):

Note These configuration examples do not protect the SSP traffic. To protect the SSP traffic, you will need to define a new crypto map and attach it to the SSP interface without the “ssp” tag. The ACL for this crypto map can be derived from the remote IP address and the TCP port that are defined in the SSP group.

```
Active# show run
Building configuration...

Current configuration : 2235 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Active
!
boot system flash sup-bootflash:
!
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
!
!
no ip domain-lookup
!
!
ssp group 100
 remote 40.0.0.2
 redundancy KNIGHTSOFNI
no mls ip multicast aggregate
no mls ip multicast non-rpf cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key NEEWOMM address 0.0.0.0 0.0.0.0
crypto isakmp ssp 100
!
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
!
crypto map ha ha replay-interval inbound 10 outbound 1000
crypto map ha 10 ipsec-isakmp
 set peer 172.16.31.3
 set transform-set TS1
 match address 101
!
!
spanning-tree extend system-id
no spanning-tree vlan 4
!
!
!
interface GigabitEthernet1/1
 no ip address
 no ip redirects
 crypto connect vlan 4
!
interface GigabitEthernet1/2
 ip address 40.0.0.1 255.255.255.0
 no ip redirects
 standby delay minimum 35 reload 60
 standby ip 40.0.0.100
 standby timers 1 3
 standby preempt
```

```
 standby track GigabitEthernet1/1
!
interface GigabitEthernet3/1
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,4,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet3/2
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 ip address 172.16.31.1 255.255.255.0
 standby delay minimum 35 reload 60
 standby ip 172.16.31.100
 standby timers 1 3
 standby preempt
 standby name KNIGHTSOFNI
 standby track GigabitEthernet1/1
 standby track GigabitEthernet1/2
 crypto map ha ssp 100
!
ip classless
ip route 10.11.1.1 255.255.255.255 172.16.31.3
no ip http server
ip pim bidir-enable
!
access-list 101 permit ip host 40.0.0.3 host 10.11.1.1
arp 127.0.0.12 0000.2100.0000 ARPA
!
!
!
line con 0
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

The following is a configuration example for the standby chassis that is configured for IPSec stateful failover:

```
StandBy# show run
Building configuration...

Current configuration : 2236 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname StandBy
!
boot system flash sup-bootflash:
!
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
!
!
no ip domain-lookup
!
!
ssp group 100
 remote 40.0.0.1
 redundancy KNIGHTSOFNI
no mls ip multicast aggregate
no mls ip multicast non-rpf cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key NEEWOMM address 0.0.0.0 0.0.0.0
crypto isakmp ssp 100
!
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
!
crypto map ha ha replay-interval inbound 10 outbound 1000
crypto map ha 10 ipsec-isakmp
 set peer 172.16.31.3
 set transform-set TS1
 match address 101
!
!
spanning-tree extend system-id
no spanning-tree vlan 4
!
!
!
interface GigabitEthernet1/1
 no ip address
 no ip redirects
 crypto connect vlan 4
!
interface GigabitEthernet1/2
 ip address 40.0.0.2 255.255.255.0
 no ip redirects
```

```
 standby delay minimum 35 reload 60
 standby ip 40.0.0.100
 standby timers 1 3
 standby preempt
 standby track GigabitEthernet1/1
!
interface GigabitEthernet3/1
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,4,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet3/2
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 ip address 172.16.31.2 255.255.255.0
 standby delay minimum 35 reload 60
 standby ip 172.16.31.100
 standby timers 1 3
 standby preempt
 standby name KNIGHTSOFNI
 standby track GigabitEthernet1/1
 standby track GigabitEthernet1/2
 crypto map ha ssp 100
!
ip classless
ip route 10.11.1.1 255.255.255.255 172.16.31.3
no ip http server
ip pim bidir-enable
!
access-list 101 permit ip host 40.0.0.3 host 10.11.1.1
arp 127.0.0.12 0000.2100.0000 ARPA
!
!
!
line con 0
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

Using IPSec NAT Transparency

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

For complete configuration information for Cisco IOS IPSec NAT transparency support, refer to this URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bca.html

There is no VPN module-specific configuration requirements or restrictions for IPSec NAT transparency. Use the standard Cisco IOS configuration that is described at the above URL.

Using TopN Acceleration

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

For complete configuration information for TopN acceleration support, refer to this URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_command_reference_chapter09186a0080132c59.html#1170304

Using IPSec Anti-Replay Window Size Expansion

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

The per-security association (SA) anti-replay window size has been increased to 64 from 32. No configuration is required to obtain the larger anti-replay window size.

Using Easy-VPN Client

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

Caution You need to clear all other crypto configurations from your running configuration on the Cisco IOS-based Easy-VPN client that you are using to connect to the VPN module. If an ISAKMP policy is configured, it takes precedence over the pre-installed Easy-VPN ISAKMP policies and the connection will fail. Other clients such as the VPN3000 and PIX systems running Easy-VPN will prevent you from configuring Easy-VPN unless all crypto configurations are removed.

For complete configuration information for Easy-VPN client support, refer to this URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide_chapter09186a00800e7251.html#xtocid2

For complete configuration information for Easy-VPN server (router side) support, refer to this URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.html

The following is a configuration example of the router-side configuration:

```
!
version 12.2
!
hostname herckt
!
boot system flash:c6sup22-jk2sv-mz
logging snmp-authfail
logging buffered 1000000 debugging
aaa new-model
aaa authentication login default local
aaa authorization network mylist local
!
username unity password 0 uc
ip subnet-zero
no ip source-route
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10 2
!
crypto isakmp client configuration group group1
 key 12345
 domain cisco.com
 pool pool1
!
crypto isakmp client configuration group default
 key 12345
 domain cisco.com
 pool pool2
!
crypto ipsec transform-set myset3 esp-3des esp-md5-hmac
!
crypto dynamic-map test_dyn 1
 set transform-set myset3
 reverse-route
!
! Static client mapping
crypto map testtag client authentication list ash
crypto map testtag isakmp authorization list groupauthor
crypto map testtag client configuration address respond
crypto map testtag 10 ipsec-isakmp
 set peer 10.5.1.4
 set security-association lifetime seconds 900
 set transform-set myset3
 match address 109
!
! Dynamic client mapping
crypto map test_dyn client authentication list ash
crypto map test_dyn isakmp authorization list groupauthor
crypto map test_dyn client configuration address respond
crypto map test_dyn 1 ipsec-isakmp dynamic test_dyn
!
!
no spanning-tree vlan 513
!
```

```
redundancy
  main-cpu
  auto-sync running-config
  auto-sync standard
!
interface GigabitEthernet2/1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,513,1002-1005
 switchport mode trunk
!
interface GigabitEthernet2/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,513,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 no ip address
 crypto connect vlan 513
!
interface Vlan513
 ip address 10.5.1.1 255.255.0.0
 crypto map test_dyn
!
ip local pool pool1 22.0.0.2
ip local pool pool2 23.0.0.3
ip classless
ip pim bidir-enable
!
access-list 109 permit ip host 10.5.1.1 host 22.0.0.2
arp 127.0.0.12 0000.2100.0000 ARPA
!
snmp-server enable traps tty
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
!
line con 0
line vty 0 4
 password lab
 transport input lat pad mop telnet rlogin udptn nasi
!
end
```

Using Dead-Peer-Detection

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

For complete configuration information for Cisco IOS Dead-Peer-Detection (DPD) support, refer to this URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide_chapter09186a00800ecb3d.html

Using WAN Interfaces

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

Follow these guidelines when configuring WAN interfaces:

- Configuring WAN interfaces is the same as configuring Ethernet routed interfaces. From the WAN subinterface, make a crypto connection to the interface VLAN as follows:

```
interface Vlan101
ip address 192.168.101.1 255.255.255.0
no mop enabled
crypto map cwan

interface ATM6/0/0.101 point-to-point
pvc 0/101
crypto connect vlan 101
```

- You must configure a crypto connection on subinterfaces for ATM and Frame Relay. For example, the following configuration will not work:

```
interface ATM6/0/0
pvc 0/101
crypto connect vlan 101
```

- For ATM and Frame Relay, there is no SVC support, no RFC-1483/1490 bridging, and no point-to-multipoint support.
- For Point-to-Point Protocol (PPP) and Multilink PPP (MLPPP), you must make the physical interface passive for routing protocols, as follows:

```
router ospf 10
        passive-interface multilink1
```

- For PPP and MLPPP, there is no Bridging Control Protocol (BCP) support.

WAN interface configuration examples are as follows:

- Crypto Connection for a Channelized T3 Port Adapter in the FlexWAN Module, page 46
- Crypto Connection for an ATM Port Adapter in the FlexWAN Module, page 47
- Crypto Connection for a POS Port Adapter in the FlexWAN Module, page 48

Crypto Connection for a Channelized T3 Port Adapter in the FlexWAN Module

The configuration for this example is as follows:

- The FlexWAN module is in slot 2.
- The channelized T3 port adapter is in bay 0.
- The VPN module is in slot 5.
- VLAN 201—serial2/0/0/1:0 (HDLC)
- VLAN 206—serial2/0/0/6:0 (PPP)
- VLAN 211—multilink1 (MLPPP)

```
!
controller T3 2/0/0
 t1 1 channel-group 0 timeslots 1-24
 t1 2 channel-group 0 timeslots 1-24
 t1 3 channel-group 0 timeslots 1-24
 t1 4 channel-group 0 timeslots 1-24
 t1 5 channel-group 0 timeslots 1-24
 t1 6 channel-group 0 timeslots 1-24
 t1 7 channel-group 0 timeslots 1-24
 t1 8 channel-group 0 timeslots 1-24
 t1 9 channel-group 0 timeslots 1-24
 t1 10 channel-group 0 timeslots 1-24
 t1 11 channel-group 0 timeslots 1-24
 t1 12 channel-group 0 timeslots 1-24
 t1 13 channel-group 0 timeslots 1-24
 t1 14 channel-group 0 timeslots 1-24
 t1 15 channel-group 0 timeslots 1-24
 t1 16 channel-group 0 timeslots 1-24
 t1 17 channel-group 0 timeslots 1-24
 t1 18 channel-group 0 timeslots 1-24
 t1 19 channel-group 0 timeslots 1-24
 t1 20 channel-group 0 timeslots 1-24
 t1 21 channel-group 0 timeslots 1-24
 t1 22 channel-group 0 timeslots 1-24
 t1 23 channel-group 0 timeslots 1-24
 t1 24 channel-group 0 timeslots 1-24
 t1 25 channel-group 0 timeslots 1-24
 t1 26 channel-group 0 timeslots 1-24
 t1 27 channel-group 0 timeslots 1-24
 t1 28 channel-group 0 timeslots 1-24
!
!
interface Multilink1
 ip unnumbered Vlan211
 no cdp enable
 ppp multilink
 multilink-group 1
 crypto connect vlan 211
!
interface Serial2/0/0/1:0
 no ip address
 no fair-queue
 no cdp enable
 crypto connect vlan 201
!
interface Serial2/0/0/6:0
 ip unnumbered Vlan206
 encapsulation ppp
 no fair-queue
 no cdp enable
```

```
 crypto connect vlan 206
!
interface Serial2/0/0/11:0
 no ip address
 encapsulation ppp
 no cdp enable
 ppp chap hostname m1
 ppp multilink
 multilink-group 1
!
interface Serial2/0/0/12:0
 no ip address
 encapsulation ppp
 no cdp enable
 ppp chap hostname m1
 ppp multilink
 multilink-group 1
!
interface Serial2/0/0/13:0
 no ip address
 encapsulation ppp
 no cdp enable
 ppp chap hostname m1
 ppp multilink
 multilink-group 1
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,201,206,211,1002-1005
 switchport mode trunk
 cdp enable
!
interface Vlan206
 ip address 192.168.206.1 255.255.255.0
 no mop enabled
!
interface Vlan211
 ip address 192.168.211.1 255.255.255.0
 no mop enabled
!
```

Crypto Connection for an ATM Port Adapter in the FlexWAN Module

The configuration for this example is as follows:

- The FlexWAN module is in slot 6.
- The ATM port adapter is in bay 0.
- The VPN module is in slot 5.
- VLAN 201—serial2/0/0/1:0 (HDLC)
- VLAN 101—ATM6/0/0.101

```
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,101,1002-1005
 switchport mode trunk
 cdp enable
!
interface ATM6/0/0
 no ip address
 atm clock INTERNAL
!
interface ATM6/0/0.101 point-to-point
 pvc 1/101
 !
 crypto connect vlan 101
!
interface Vlan101
 ip address 192.168.101.1 255.255.255.0
 no mop enabled
!
```

Crypto Connection for a POS Port Adapter in the FlexWAN Module

The configuration for this example is as follows:

- The FlexWAN module is in slot 6.
- The POS port adapter is in bay 1.
- The VPN module is in slot 5.
- VLAN 16—pos6/1/0.16

```
!
frame-relay switching
!
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface POS6/1/0
 no ip address
 encapsulation frame-relay
!!!
!!! The peer POS interface config does not need
!!! to have the following two lines.
!!!
 no keepalive
 clock source internal
 frame-relay intf-type dce
!
interface POS6/1/0.16 point-to-point
 no cdp enable
 frame-relay interface-dlci 16
```

```
 crypto connect vlan 16
!
interface Vlan16
 ip address 192.168.16.1 255.255.255.0
 no mop enabled
```

Using Look-Ahead Fragmentation

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

Follow these guidelines for using Look-Ahead Fragmentation (LAF):

- Large packets can increase the IPSec packet size beyond the MTU causing the IPSec packets to be fragmented. When this situation occurs, the receiving IPSec peer must reassemble the packets prior to decryption. This action can cause serious loading for many VPN gateway devices. The solution is to fragment the packets before IPSec decryption and let the end devices bear the reassembly load.
- If there is no large packet connectivity through an IPSec peer, turn off LAF (the peer may be discarding fragments found inside the IPSec packets).
- If an IPSec peer is experiencing high CPU utilization with large packet flows, verify that LAF is enabled (the peer may be reassembling large packets).

For complete configuration information for LAF, refer to this URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080115533.html

Using GRE Tunneling

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

Note The VPN module is able to accelerate packet processing for up to 1023 GRE tunnels per chassis; excess tunnels go through the route processor. The switch supports any number of GRE tunnels, but adding more VPN modules does not increase the 1023 tunnels per-chassis maximum.

In Catalyst 6500 series switches or Cisco 7600 Series Internet Routers, GRE encapsulation and decapsulation is traditionally performed by the route processor. When routing indicates that encapsulated packets for a GRE tunnel will egress through an interface VLAN that is attached to a VPN module inside port, that VPN module will seize the GRE tunnel. By seizing the tunnel, the VPN module takes the GRE encapsulation and decapsulation duty from the route processor.

No explicit configuration changes are required to use this feature; configure GRE as you normally would. As long as routing sends the GRE-encapsulated packets out an interface VLAN, the VPN module will seize the GRE tunnel.

Follow these guidelines for configuring GRE tunneling:

- If routing information changes and the GRE-encapsulated packets no longer egress through an interface VLAN, the VPN module yields the GRE tunnel. After the VPN module yields the tunnel, the route processor resumes encapsulation and decapsulation which increases CPU utilization on the route processor.

Caution Ensure that your GRE tunnel configuration does not overload the route processor.

  In Cisco IOS Release 12.2(9)YO and additional YO builds, all GRE encapsulation was performed on the route processor. In Cisco IOS Release 12.2(14)SY, GRE tunnels that egress through a VPN module have their GRE encapsulation and decapsulation performed by the VPN module. This offloads the route processor from packet-processing tasks and also allows GRE scaling with additional VPN modules.

- A delay occurs (up to 10 seconds) between routing changes and the VPN module seizing the GRE tunnel.
- When packets that are destined to a GRE tunnel arrive from a switching module that has a DFC daughter card installed, GRE encapsulation is done by the route processor. The packets do not reach the VPN module. The Cisco IOS software encapsulates the packets with the GRE header and then sends them to the VPN module. When this occurs, the GRE performance is limited by the software. If the switching module does not have the DFC card, there is no issue and the VPN module encapsulates the packets.
- If you are switching between hardware and software-based cryptographic modes, it is important to note that the crypto map must only be applied to the interface VLAN and not to the tunnel interface. This restriction is different from a software-based cryptographic mode where you attach the crypto map to the physical (or VLAN) interface *and* to the tunnel interface.
- Tunnel mode is the only GRE mode that is supported. You may use the **ttl** and **tos** options with the tunnel mode.
- The following options are not supported: **sequence**, **key**, and **checksum**. If any of these options are specified, the VPN module will not seize the GRE tunnel.
- Use the **show crypto vlan** command to verify that the VPN module has seized the GRE tunnel:

```
Router-2# show crypto vlan
Interface VLAN 101 on IPSec Service Module port 7/1 connected to AT4/0/0.101
    Tunnel101 is accelerated via IPSec SM in slot 7
Router-2#
```

- GRE tunneling of all non-IP packets is done by the route processor even if the tunnel is seized by the VPN module.
- Configuring “service policy” on GRE tunnel interfaces is not supported.

For GRE tunneling configuration examples, see the “GRE Tunneling” section on page 86.

Using QoS

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

The VPN module uses the QoS capabilities of the Catalyst 6500 series switches and Cisco 7600 Series Internet Router software. Before configuring QoS for the VPN module, refer to this URL:

http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008014a29f.shtml

The VPN module supports two-level, strict-priority QoS (high priority versus low priority). To take advantage of the VPN module's QoS capability, you must use standard QoS commands to ensure that the CoS of packets are marked on ingress. You must configure the CoS map for the VPN module inside and outside ports. The VPN module behaves according to the settings of the inside and outside ports. You must enable QoS globally for the VPN module to acknowledge the CoS mapping.

For example, if the CoS map of the inside and outside ports map CoS value 5 to the high-priority queue and you have globally enabled QoS, the VPN module will give traffic marked CoS 5 higher priority than traffic marked with any of the other seven CoS values. If you alter the CoS map of the inside and outside ports so that CoS 6 additionally maps to the high-priority queue, then packets marked with either CoS 5 or CoS 6 will be given higher priority within the VPN module.

As many as three high-priority CoS map values are supported per VPN module. When global QoS is enabled, the CoS value of 5 is preconfigured. This allows you to add only two more values in addition to the preconfigured CoS 5 value. For QoS configuration examples, see the "QoS" section on page 94.

Port Configuration Procedures

These sections describe how to configure the VPN module:

Note The procedures in this section do not provide detailed information on configuring the following Cisco IOS features: IKE policies, preshared key entries, Cisco IOS ACLs, and crypto maps. For detailed information on configuring these features, refer to the following Cisco IOS documentation:

Cisco IOS Security Configuration Guide, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm

Cisco IOS Security Command Reference, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

Configuring a VPN Access Port Connection

This section describes how to configure the VPN module with an access port connection to the WAN router (see Figure 10).

Note In the following example, the VPN module is installed in slot 5 (Gigabit Ethernet interfaces 5/1 and 5/2).

To configure an access port connection to the WAN router, follow these steps:

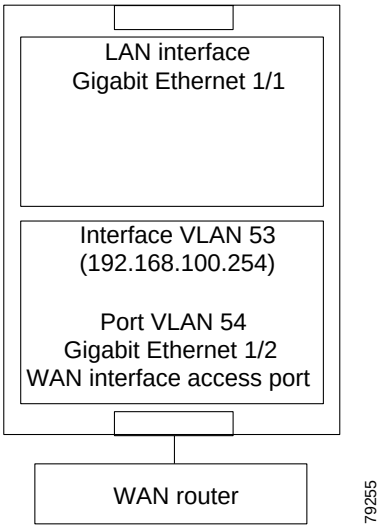
Step 1 Create an IKE policy, if necessary.

Step 2 Create a preshared key entry, if necessary.

Step 3 Create an ACL.

Step 4 Create a crypto map.

Figure 10 Access Port Configuration Example



Step 5 From privileged EXEC mode, add an *inside* interface VLAN (VLAN 53) and an *outside* access port VLAN (VLAN 54) to the VLAN database as follows:

a. Router# **config t**

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Router(config)# **vlan 53**

Router(config-vlan)# **name inside_interface_vlan**

Router(config-vlan)# **exit**

Router(config)#

c. Router(config)# **vlan 54**

Router(config-vlan)# **name outside_access_port_vlan**

Router(config-vlan)# **exit**

Router(config)#

Step 6 From interface configuration mode, create a Layer 3 inside interface VLAN and attach a crypto map as follows:

a. Router# **config t**

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Router(config)# **interface vlan 53**

c. Router(config-if)# **description inside_interface_vlan_for_crypto_map**

d. Router(config-if)# **ip address 192.168.100.254 255.255.255.0**

e. Router(config-if)# **crypto map map101**

f. Router(config-if)# **no shutdown**

Step 7 From interface configuration mode, create an outside interface VLAN for the outside access port VLAN as follows:

a. Router(config)# **interface vlan 54**

b. Router(config-if)# **description outside_interface_vlan_for_outside_access_vlan**

c. Router(config-if)# **no shutdown**

Step 8 From interface configuration mode, add inside interface VLAN 53 as an allowed VLAN as follows:

a. Router(config-if)# **interface gigabitethernet 5/1**

b. Router(config-if)# **description inside_vpn_module_trunk_port**

c. Router(config-if)# **switchport trunk allowed vlan add 53**

Step 9 From interface configuration mode, add switch port 1/2 to the outside access port VLAN and connect the outside access port VLAN to the inside interface VLAN as follows:

Router(config-if)# **interface gigabitethernet 1/2**

Router(config-if)# **description outside_vlan_access_port**

Router(config-if)# **switchport**

Router(config-if)# **switchport access vlan 54**

Router(config-if)# **crypto connect vlan 53**

Configuring a VPN Routed Port Connection

This section describes how to configure the VPN module with a routed port connection to the WAN router (see Figure 11).

Note A routed port uses a hidden VLAN.

Note In the following example, the VPN module is installed in slot 5 (Gigabit Ethernet interfaces 5/1 and 5/2).

To configure a routed port connection to the WAN router, follow these steps:

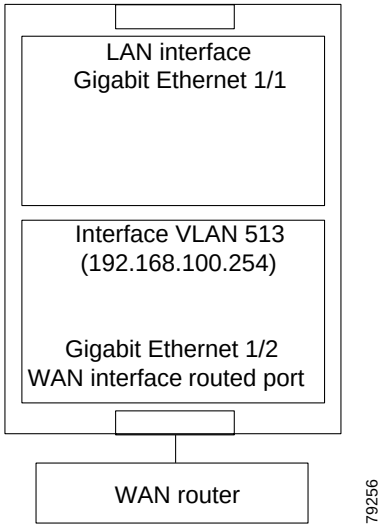
Step 1 Create an IKE policy, if necessary.

Step 2 Create a preshared key entry, if necessary.

Step 3 Create an ACL.

Step 4 Create a crypto map.

Figure 11 Routed Port Configuration Example



Step 5 From privileged EXEC mode, add an *inside* interface VLAN to the VLAN database as follows:

a. Router# **config t**

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Router(config)# **vlan 513**

Router(config-vlan)# **name inside_interface_vlan**

Router(config-vlan)# **exit**

Router(config)#

Step 6 From interface configuration mode, create a Layer 3 inside interface VLAN and attach a crypto map as follows:

a. Router# **config t**

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Router(config)# **interface vlan 513**

c. Router(config-if)# **description inside_interface_vlan_for_crypto_map**

d. Router(config-if)# **ip address 192.168.100.254 255.255.255.0**

e. Router(config-if)# **crypto map map101**

f. Router(config-if)# **no shutdown**

Step 7 From interface configuration mode, add inside interface VLAN 513 as an allowed VLAN as follows:

a. Router(config-if)# **interface gigabitethernet 5/1**

b. Router(config-if)# **description inside_vpn_module_trunk_port**

c. Router(config-if)# **switchport trunk allowed vlan add 513**

Step 8 From interface configuration mode, connect the routed port to the inside interface VLAN as follows:

Router(config-if)# **interface gigabitethernet 1/2**

Router(config-if)# **description outside_vlan_access_port**

Router(config-if)# **crypto connect vlan 513**

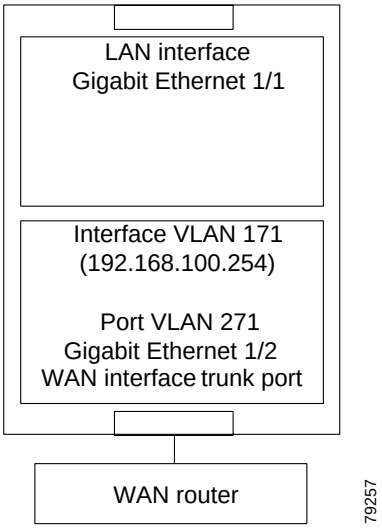
Configuring a VPN Trunk Port Connection

Caution When you configure an Ethernet port as a trunk port, all the VLANs are allowed on the trunk port by default. This default configuration does not work well with the VPN module and causes network loops. For detailed information on configuring trunks, see the "Trunks" section in the "Interaction with Other Features" section on page 25.

This section describes how to configure the VPN module with a trunk port connection to the WAN router (see Figure 12).

Note In the following example, the VPN module is installed in slot 5 (Gigabit Ethernet interfaces 5/1 and 5/2).

Figure 12 Trunk Port Configuration Example



To configure a trunk port connection to the WAN router, follow these steps:

Step 1 Create an IKE policy, if necessary.

Step 2 Create a preshared key entry, if necessary.

Step 3 Create an ACL.

Step 4 Create a crypto map.

Step 5 From privileged EXEC mode, add an *inside* interface VLAN (VLAN 171) and an *outside* trunk port VLAN (VLAN 271) to the VLAN database as follows:

a. Router# **config t**

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Router(config)# **vlan 171**

Router(config-vlan)# **name inside_interface_vlan**

Router(config-vlan)# **exit**

Router(config)#

c. Router(config)# **vlan 271**

Router(config-vlan)# **name outside_trunk_port_vlan**

Router(config-vlan)# **exit**

Router(config)#

Step 6 From interface configuration mode, create a Layer 3 inside interface VLAN and attach a crypto map as follows:

a. Router# **config t**

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Router(config)# **interface vlan 171**

c. Router(config-if)# **description inside_interface_vlan_for_crypto_map**

d. Router(config-if)# **ip address 192.168.100.254 255.255.255.0**

e. Router(config-if)# **crypto map map101**

f. Router(config-if)# **no shutdown**

Step 7 From interface configuration mode, add inside interface VLAN 171 as an allowed VLAN as follows:

Router(config)# **interface gigabitethernet 5/1**

Router(config-if)# **description inside_vpn_module_trunk_port**

Router(config-if)# **switchport trunk allowed vlan add 171**

Step 8 From interface configuration mode, create the outside trunk port VLAN interface and connect it to the inside interface VLAN as follows:

a. Router(config)# **interface vlan 271**

b. Router(config-if)# **description outside_trunk_port_vlan**

c. Router(config-if)# **crypto connect vlan 171**

d. Router(config-if)# **no shutdown**

Step 9 From interface configuration mode, configure a trunked switch port and add the outside trunk port VLAN (VLAN 271) as an allowed VLAN as follows:

a. Router(config)# **interface gigabitethernet 1/2**

b. Router(config-if)# **description outside_trunk_port_vlan**

c. Router(config-if)# **switchport**

d. Router(config-if)# **no switchport access vlan**

e. Router(config-if)# **switchport trunk encapsulation dot1q**

f. Router(config-if)# **switchport mode trunk**

g. Router(config-if)# **switchport trunk allowed vlan remove 2-1001**

h. Router(config-if)# **switchport trunk allowed vlan add 271**

Displaying the VPN Running State

Use the **show crypto vlan** command to display the VPN running state. The following examples show the **show crypto vlan** command output for a variety of VPN module configurations:

Router# **show crypto vlan**

```
Interface VLAN 2 on IPSec Service Module port 7/1 connected to Fa8/3
```

Router# **show crypto vlan**

```
Interface VLAN 2 on IPSec Service Module port 7/1 connected to VLAN 3
```

Router# **show crypto vlan**

```
Interface VLAN 2 connected to VLAN 3 (no IPSec Service Module attached)
```

The above display indicates that either the interface VLAN is missing on the VPN module inside port, the VPN module is removed from the chassis, or the VPN module was moved to a different slot.

Configuration Examples

These sections provide examples for the following configurations:

Access Ports

These sections describe access port configuration:

Note In the following example, the VPN module is installed in slot 5 (Gigabit Ethernet interfaces 5/1 and 5/2).

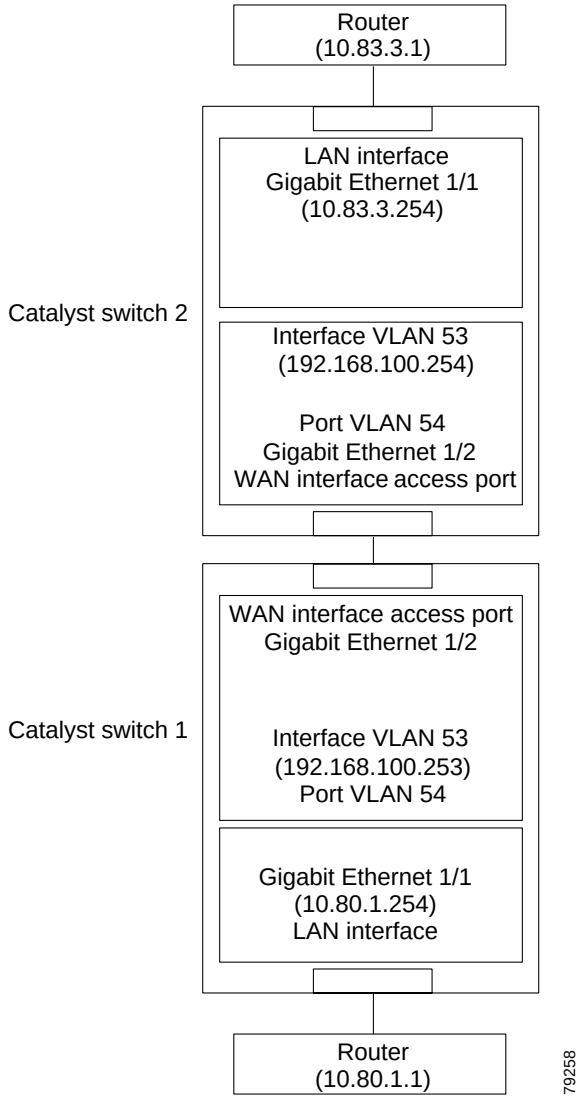
Catalyst Switch 1 (Access Port)

The Catalyst switch 1 configuration is as follows (see Figure 13):

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-1
!
boot system flash:c6sup22-jk2sv-mz
!
redundancy
 main-cpu
  auto-sync standard
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Jolly-Good-Fellow address 192.168.100.254
!
!
crypto ipsec transform-set TS-101 esp-3des esp-sha-hmac
!
crypto map MAP-101 10 ipsec-isakmp
 set peer 192.168.100.254
 set security-association lifetime kilobytes 10000
 set security-association lifetime seconds 86000
 set transform-set TS-101
 match address AEO-101
!
!
no spanning-tree vlan 53
!
!
!
interface GigabitEthernet1/1
 ip address 10.80.1.254 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport access vlan 54
 switchport mode access
 no ip address
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,53,1002-1005
 switchport mode trunk
```

```
 no ip address
 flowcontrol receive on
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,54,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan53
 ip address 192.168.100.253 255.255.255.0
 crypto map MAP-101
!
interface Vlan54
 no ip address
 crypto connect vlan 53
!
ip classless
ip route 10.83.3.0 255.255.255.0 192.168.100.254
no ip http server
!
!
ip access-list extended AEO-101
 permit ip 10.80.0.0 0.0.255.255 10.83.0.0 0.0.255.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Figure 13 Access Port Configuration Example



Catalyst Switch 2 (Access Port)

The Catalyst switch 2 configuration is as follows (see Figure 13):

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-2
!
boot system flash:c6sup22-jk2sv-mz
!
redundancy
 main-cpu
  auto-sync standard
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Jolly-Good-Fellow address 192.168.100.253
!
!
crypto ipsec transform-set TS-101 esp-3des esp-sha-hmac
!
crypto map MAP-101 10 ipsec-isakmp
 set peer 192.168.100.253
 set security-association lifetime kilobytes 10000
 set security-association lifetime seconds 86000
 set transform-set TS-101
 match address AEO-101
!
!
no spanning-tree vlan 53
!
!
!
interface GigabitEthernet1/1
 ip address 10.83.3.254 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport access vlan 54
 switchport mode access
 no ip address
!
```

```
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,53,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,54,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan53
 ip address 192.168.100.254 255.255.255.0
 crypto map MAP-101
!
interface Vlan54
 no ip address
crypto connect vlan 53
!
ip classless
ip route 10.80.1.0 255.255.255.0 192.168.100.253
no ip http server
!
!
ip access-list extended AEO-101
 permit ip 10.83.0.0 0.0.255.255 10.80.0.0 0.0.255.255
!
!
line con 0
line vty 0
 login
!
end
```

Routed Ports

These sections describe routed port configuration:

- Catalyst Switch 1 (Routed Port), page 64
- Catalyst Switch 2 (Routed Port), page 66

Note In the following example, the VPN module is installed in slot 5 (Gigabit Ethernet interfaces 5/1 and 5/2).

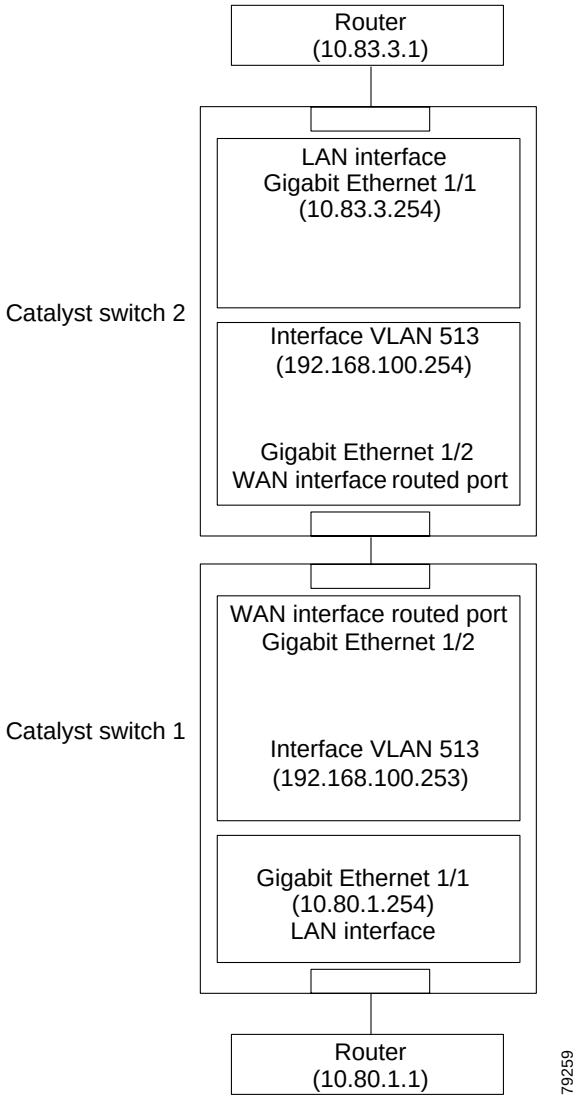
Catalyst Switch 1 (Routed Port)

The Catalyst switch 1 configuration is as follows (see Figure 14):

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-1
!
boot system flash:c6sup22-jk2sv-mz
!
redundancy
 main-cpu
  auto-sync standard
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Jolly-Good-Fellow address 192.168.100.254
!
!
crypto ipsec transform-set TS-101 esp-3des esp-sha-hmac
!
crypto map MAP-101 10 ipsec-isakmp
 set peer 192.168.100.254
 set security-association lifetime kilobytes 10000
 set security-association lifetime seconds 86000
 set transform-set TS-101
 match address AEO-101
!
!
!
!
interface GigabitEthernet1/1
 ip address 10.80.1.254 255.255.255.0
!
interface GigabitEthernet1/2
 no ip address
 crypto connect vlan 513
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,513,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
```

```
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan513
 ip address 192.168.100.253 255.255.255.0
 crypto map MAP-101
!
ip classless
ip route 10.83.3.0 255.255.255.0 192.168.100.254
no ip http server
!
!
ip access-list extended AEO-101
 permit ip 10.80.0.0 0.0.255.255 10.83.0.0 0.0.255.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Figure 14 Routed Port Configuration Example



Catalyst Switch 2 (Routed Port)

The Catalyst switch 2 configuration is as follows (see Figure 14):

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-2
!
boot system flash:c6sup22-jk2sv-mz
!
```

```
redundancy
 main-cpu
  auto-sync standard
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Jolly-Good-Fellow address 192.168.100.253
!
!
crypto ipsec transform-set TS-101 esp-3des esp-sha-hmac
!
crypto map MAP-101 10 ipsec-isakmp
 set peer 192.168.100.253
 set security-association lifetime kilobytes 10000
 set security-association lifetime seconds 86000
 set transform-set TS-101
 match address AEO-101
!
!
!
!
interface GigabitEthernet1/1
 ip address 10.83.3.254 255.255.255.0
!
interface GigabitEthernet1/2
 no ip address
 crypto connect vlan 513
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,513,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
```

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan513
 ip address 192.168.100.254 255.255.255.0
 crypto map MAP-101
!
ip classless
ip route 10.80.1.0 255.255.255.0 192.168.100.253
no ip http server
!
!
ip access-list extended AEO-101
 permit ip 10.83.0.0 0.0.255.255 10.80.0.0 0.0.255.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Trunk Ports

These sections describe trunk port configuration:

- Catalyst Switch 1 (Trunk Port), page 68
- Catalyst Switch 2 (Trunk Port), page 71

Note In the following example, the VPN module is installed in slot 5 (Gigabit Ethernet interfaces 5/1 and 5/2).

Catalyst Switch 1 (Trunk Port)

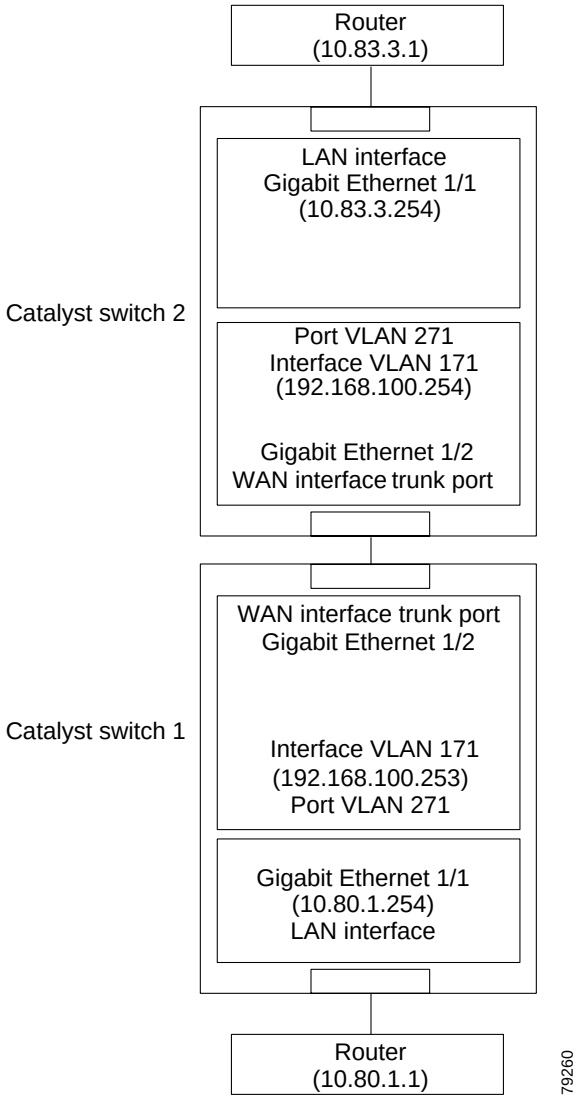
The Catalyst switch 1 configuration is as follows (see Figure 15):

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-1
!
boot system flash:c6sup22-jk2sv-mz
!
redundancy
 main-cpu
  auto-sync standard
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
```

```
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Jolly-Good-Fellow address 192.168.100.254
!
!
crypto ipsec transform-set TS-101 esp-3des esp-sha-hmac
!
crypto map MAP-101 10 ipsec-isakmp
 set peer 192.168.100.254
 set security-association lifetime kilobytes 10000
 set security-association lifetime seconds 86000
 set transform-set TS-101
 match address AEO-101
!
!
no spanning-tree vlan 171
!
!
!
interface GigabitEthernet1/1
 ip address 10.80.1.254 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,271,1002-1005
 switchport mode trunk
 no ip address
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,171,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,271,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan171
 ip address 192.168.100.253 255.255.255.0
 crypto map MAP-101
!
interface Vlan271
 no ip address
 crypto connect vlan 171
!
ip classless
ip route 10.83.3.0 255.255.255.0 192.168.100.254
no ip http server
```

```
!
!
ip access-list extended AEO-101
 permit ip 10.80.0.0 0.0.255.255 10.83.0.0 0.0.255.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Figure 15 Trunk Port Configuration Example



Catalyst Switch 2 (Trunk Port)

The Catalyst switch 2 configuration is as follows (see Figure 15):

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-2
!
boot system flash:c6sup22-jk2sv-mz
!
redundancy
 main-cpu
  auto-sync standard
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Jolly-Good-Fellow address 192.168.100.253
!
!
crypto ipsec transform-set TS-101 esp-3des esp-sha-hmac
!
crypto map MAP-101 10 ipsec-isakmp
 set peer 192.168.100.253
 set security-association lifetime kilobytes 10000
 set security-association lifetime seconds 86000
 set transform-set TS-101
 match address AEO-101
!
!
no spanning-tree vlan 171
!
!
!
interface GigabitEthernet1/1
 ip address 10.83.3.254 255.255.255.0
!
interface GigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,271,1002-1005
 switchport mode trunk
 no ip address
!
```

```
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,171,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,271,1002-1005
 switchport mode trunk
 no ip address
 flowcontrol receive on
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan171
 ip address 192.168.100.254 255.255.255.0
 crypto map MAP-101
!
interface Vlan271
 no ip address
 crypto connect vlan 171
!
ip classless
ip route 10.80.1.0 255.255.255.0 192.168.100.253
no ip http server
!
!
ip access-list extended AEO-101
 permit ip 10.83.0.0 0.0.255.255 10.80.0.0 0.0.255.255
!
!
line con 0
line vty 0 4
 login
!
end
```

ATM Ports

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

These sections describe ATM port configuration:

Catalyst Switch 1 (ATM Port)

The Catalyst switch 1 configuration is as follows:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname Router-1
!
boot system flash bootflash:c6k
logging snmp-authfail
enable password lab
!
vtp mode transparent
ip subnet-zero
!
!
no ip domain-lookup
ip host tftp-serv 10.80.1.1
ip host tftp 10.80.1.1
ip host ockham 172.16.1.1
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key foobar address 192.168.0.0 255.255.0.0
!
!
crypto ipsec transform-set ts-cwan esp-3des esp-sha-hmac
!
crypto map cwan-101 10 ipsec-isakmp
 set peer 192.168.101.2
 set transform-set ts-cwan
 match address acl-101
!
!
no spanning-tree vlan 6,101
!
redundancy
  main-cpu
  auto-sync running-config
```

```
  auto-sync standard
!
controller T3 2/0/0
 t1 1 channel-group 0 timeslots 1-24
 t1 2 channel-group 0 timeslots 1-24
 .
 .
 .
 t1 27 channel-group 0 timeslots 1-24
 t1 28 channel-group 0 timeslots 1-24
!
!
vlan 1
 tb-vlan1 1002
 tb-vlan2 1003
!
vlan 2-1001
!
vlan 1002
 tb-vlan1 1
 tb-vlan2 1003
!
vlan 1003
 tb-vlan1 1
 tb-vlan2 1002
 backupcrf enable
!
vlan 1004
 bridge 1
 stp type ibm
!
!
interface Loopback7
 ip address 7.7.7.7 255.255.255.255
!
interface Multilink1
 no ip address
 no cdp enable
 ppp multilink
 multilink-group 1
.
.
.
interface Multilink6
 no ip address
 no cdp enable
 ppp multilink
 multilink-group 6
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 mtu 4500
 ip address 11.22.1.1 255.255.255.0
 speed nonegotiate
 no cdp enable
!
interface Serial2/0/0/1:0
 ip unnumbered Loopback7
 encapsulation ppp
 no fair-queue
 no cdp enable
```

```
 crypto connect vlan 6
!
interface Serial2/0/0/2:0
 no ip address
 no fair-queue
 no cdp enable
.
.
.
interface Serial2/0/0/27:0
 no ip address
 no fair-queue
 no cdp enable
!
interface Serial2/0/0/28:0
 no ip address
 no fair-queue
 no cdp enable
!
interface FastEthernet3/1
 ip address 10.80.1.254 255.255.255.0
 no cdp enable
!
interface FastEthernet3/2
 no ip address
 shutdown
.
.
.
!
interface FastEthernet3/38
 no ip address
 shutdown
!
interface FastEthernet3/39
 ip address 3.5.39.7 255.255.255.0
 no cdp enable
!
interface FastEthernet3/40
 ip address 3.5.40.7 255.255.255.0
 no cdp enable
!
interface FastEthernet3/41
 no ip address
 shutdown
.
.
.
!
interface FastEthernet3/47
 ip address 172.16.1.254 255.255.255.0
 no cdp enable
!
interface FastEthernet3/48
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,6,101,1002-1005
 switchport mode trunk
```

```
 cdp enable
!
interface GigabitEthernet5/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
!
interface ATM6/0/0
 no ip address
 atm clock INTERNAL
!
interface ATM6/0/0.101 point-to-point
 pvc 0/101
 crypto connect vlan 101
!
interface POS6/1/0
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan6
 ip address 192.168.6.1 255.255.255.0
 no mop enabled
!
interface Vlan101
 ip address 192.168.101.1 255.255.255.0
 no mop enabled
 crypto map cwan-101
!
router eigrp 6
 network 192.168.6.0
 auto-summary
!
ip classless
ip route 10.10.20.101 255.255.255.255 192.168.101.2
no ip http server
!
!
ip access-list extended acl-101
 permit ip host 172.16.1.101 host 10.10.20.101
!
no cdp run
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password lab
 no login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
scheduler runtime netinput 300
end
```

Catalyst Switch 2 (ATM Port)

The Catalyst switch 2 configuration is as follows:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-2
!
boot system flash bootflash:c6k
logging snmp-authfail
enable password lab
!
ip subnet-zero
!
!
no ip domain-lookup
ip host charles 10.10.20.1
ip host tftp 223.255.254.254
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key foobar address 192.168.0.0 255.255.0.0
!
!
crypto ipsec transform-set ts-cwan esp-3des esp-sha-hmac
!
crypto map cwan-101 10 ipsec-isakmp
 set peer 192.168.101.1
 set transform-set ts-cwan
 match address acl-101
!
!
no spanning-tree vlan 101
!
redundancy
  main-cpu
  auto-sync running-config
  auto-sync standard
!
controller T3 3/0/0
 t1 1 channel-group 0 timeslots 1-24
 t1 2 channel-group 0 timeslots 1-24
 .
 .
 .
 t1 27 channel-group 0 timeslots 1-24
 t1 28 channel-group 0 timeslots 1-24
!
!
!
interface Multilink1
 no ip address
 ppp multilink
```

```
 multilink-group 1
.
.
.
!
interface Multilink6
 no ip address
 ppp multilink
 multilink-group 6
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface Serial3/0/0/1:0
 no ip address
 no fair-queue
.
.
.
!
interface Serial3/0/0/28:0
 no ip address
 no fair-queue
!
interface ATM4/0/0
 no ip address
 atm clock INTERNAL
!
interface ATM4/0/0.101 point-to-point
 pvc 0/101
 crypto connect vlan 101
!
interface POS4/1/0
 no ip address
 shutdown
!
interface GigabitEthernet7/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,101,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet7/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet8/1
 no ip address
 shutdown
!
interface FastEthernet8/2
```

```
 ip address 10.10.20.254 255.255.255.0
!
interface FastEthernet8/3
 no ip address
 shutdown
.
.
.
!
interface FastEthernet8/47
 no ip address
 shutdown
!
interface FastEthernet8/48
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan101
 ip address 192.168.101.2 255.255.255.0
 no mop enabled
 crypto map cwan-101
!
ip classless
ip route 172.16.1.101 255.255.255.255 192.168.101.1
no ip http server
no ip http secure-server
!
!
ip access-list extended acl-101
 permit ip host 10.10.20.101 host 172.16.1.101
!
!
line con 0
 exec-timeout 0 0
line vty 0 4
 no login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

Frame Relay Ports

Note This section applies to VPN modules running Cisco IOS Release 12.2(14)SY or later releases.

These sections describe Frame Relay port configuration:

- Catalyst Switch 1 (Frame Relay Port), page 80
- Catalyst Switch 2 (Frame Relay Port), page 83

Catalyst Switch 1 (Frame Relay Port)

The Catalyst switch 1 configuration is as follows:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname Router-1
!
boot system flash bootflash:c6k
logging snmp-authfail
enable password lab
!
vtp mode transparent
ip subnet-zero
!
!
no ip domain-lookup
ip host ockham 172.16.1.1
ip host tftp 10.80.1.1
ip host tftp-serv 10.80.1.1
!
frame-relay switching
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key foobar address 192.168.0.0 255.255.0.0
!
!
crypto ipsec transform-set ts-cwan esp-3des esp-sha-hmac
!
crypto map cwan-16 10 ipsec-isakmp
 set peer 192.168.16.2
 set transform-set ts-cwan
 match address acl-16
!
!
no spanning-tree vlan 16
!
redundancy
  main-cpu
  auto-sync running-config
  auto-sync standard
!
controller T3 2/0/0
 t1 1 channel-group 0 timeslots 1-24
 t1 2 channel-group 0 timeslots 1-24
 .
 .
 .
 t1 27 channel-group 0 timeslots 1-24
 t1 28 channel-group 0 timeslots 1-24
!
!
```

```
vlan 1
 tb-vlan1 1002
 tb-vlan2 1003
!
vlan 2-1001
!
vlan 1002
 tb-vlan1 1
 tb-vlan2 1003
!
vlan 1003
 tb-vlan1 1
 tb-vlan2 1002
 backupcrf enable
!
vlan 1004
 bridge 1
 stp type ibm
!
!
interface Multilink1
 no ip address
 no cdp enable
 ppp multilink
 multilink-group 1
.
.
.
!
interface Multilink6
 no ip address
 no cdp enable
 ppp multilink
 multilink-group 6
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 mtu 4500
 ip address 11.22.1.1 255.255.255.0
 speed nonegotiate
 no cdp enable
!
interface Serial2/0/0/1:0
 no ip address
 no fair-queue
 no cdp enable
.
.
.
!
interface Serial2/0/0/28:0
 no ip address
 no fair-queue
 no cdp enable
!
interface FastEthernet3/1
 ip address 10.80.1.254 255.255.255.0
 no cdp enable
!
```

```
interface FastEthernet3/2
 no ip address
 shutdown
.
.
.
!
interface FastEthernet3/38
 no ip address
 shutdown
!
interface FastEthernet3/39
 ip address 3.5.39.7 255.255.255.0
 no cdp enable
!
interface FastEthernet3/40
 ip address 3.5.40.7 255.255.255.0
 no cdp enable
!
interface FastEthernet3/41
 no ip address
 shutdown
.
.
.
!
interface FastEthernet3/46
 no ip address
 shutdown
!
interface FastEthernet3/47
 ip address 172.16.1.254 255.255.255.0
 no cdp enable
!
interface FastEthernet3/48
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet5/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
!
interface ATM6/0/0
 no ip address
 shutdown
!
interface POS6/1/0
 no ip address
 encapsulation frame-relay
 no keepalive
```

```
 clock source internal
 frame-relay intf-type dce
!
interface POS6/1/0.16 point-to-point
 no cdp enable
 frame-relay interface-dlci 16
 crypto connect vlan 16
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan16
 ip address 192.168.16.1 255.255.255.0
 no mop enabled
 crypto map cwan-16
!
ip classless
ip route 10.10.20.16 255.255.255.255 192.168.16.2
no ip http server
no ip http secure-server
!
!
ip access-list extended acl-16
 permit ip host 172.16.1.16 host 10.10.20.16
!
no cdp run
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password lab
 no login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
scheduler runtime netinput 300
end
```

Catalyst Switch 2 (Frame Relay Port)

The Catalyst switch 2 configuration is as follows:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router-2
!
boot system flash bootflash:c6k
logging snmp-authfail
enable password lab
!
ip subnet-zero
!
!
no ip domain-lookup
ip host charles 10.10.20.1
ip host tftp 223.255.254.254
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
```

```
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key foobar address 192.168.0.0 255.255.0.0
!
!
crypto ipsec transform-set ts-cwan esp-3des esp-sha-hmac
!
crypto map cwan-16 10 ipsec-isakmp
 set peer 192.168.16.1
 set transform-set ts-cwan
 match address acl-16
!
!
no spanning-tree vlan 16
!
redundancy
  main-cpu
  auto-sync running-config
  auto-sync standard
!
controller T3 3/0/0
 t1 1 channel-group 0 timeslots 1-24
 t1 2 channel-group 0 timeslots 1-24
 .
 .
 .
 t1 27 channel-group 0 timeslots 1-24
 t1 28 channel-group 0 timeslots 1-24
!
!
!
interface Multilink1
 no ip address
 ppp multilink
 multilink-group 1
.
.
.
!
interface Multilink6
 no ip address
 ppp multilink
 multilink-group 6
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface Serial3/0/0/1:0
 no ip address
 no fair-queue
.
.
.
!
interface Serial3/0/0/28:0
```

```
 no ip address
 no fair-queue
!
interface ATM4/0/0
 no ip address
 shutdown
!
interface POS4/1/0
 no ip address
 encapsulation frame-relay
 no keepalive
 clock source internal
!
interface POS4/1/0.16 point-to-point
 frame-relay interface-dlci 16
 crypto connect vlan 16
!
interface GigabitEthernet7/1
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet7/2
 no ip address
 flowcontrol receive on
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet8/1
 no ip address
 shutdown
!
interface FastEthernet8/2
 ip address 10.10.20.254 255.255.255.0
!
interface FastEthernet8/3
 no ip address
 shutdown
.
.
.
!
interface FastEthernet8/48
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan16
 ip address 192.168.16.2 255.255.255.0
 no mop enabled
 crypto map cwan-16
!
ip classless
ip route 172.16.1.16 255.255.255.255 192.168.16.1
```

```
no ip http server
no ip http secure-server
!
!
ip access-list extended acl-16
 permit ip host 10.10.20.16 host 172.16.1.16
!
!
line con 0
 exec-timeout 0 0
line vty 0 4
 no login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

GRE Tunneling

These sections provide examples for GRE tunneling:

- Catalyst Switch 1, page 86
- Catalyst Switch 2, page 87

Note In both switches, the VPN module is in slot 5, Gigabit Ethernet interfaces 1/1 are the secured ports, and Gigabit Ethernet interfaces 1/2 are the LAN ports.

Catalyst Switch 1

The Catalyst switch 1 configuration is as follows:

```
crypto isakmp policy 100
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 192.168.1.0 255.255.255.0
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
!
crypto map cm1 100 ipsec-isakmp
 set peer 192.168.1.1
 set security-association level per-host
 set security-association lifetime kilobytes 536870912
 set security-association lifetime seconds 86400
 set transform-set ts
 match address acl1
!
interface GigabitEthernet1/1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
!
interface GigabitEthernet1/2
 ip address 5.0.0.254 255.255.255.0
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
```

```
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 cdp enable
!
interface Vlan2
 ip address 192.168.1.254 255.255.255.0
 no mop enabled
 crypto map cm1
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Tunnel1
 ip address 10.1.1.254 255.255.255.0
 tunnel source vlan1
 tunnel destination 192.168.1.1
!
ip route 6.0.0.0 255.255.255.0 Tunnel1
!
ip access-list extended acl1
 permit gre host 192.168.1.254 host 192.168.1.1
!
```

Catalyst Switch 2

The Catalyst switch 2 configuration is as follows:

```
crypto isakmp policy 100
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 192.168.1.0 255.255.255.0
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
!
crypto map cm1 100 ipsec-isakmp
 set peer 192.168.1.254
 set security-association level per-host
 set security-association lifetime kilobytes 536870912
 set security-association lifetime seconds 86400
 set transform-set ts
 match address acl1
!
interface GigabitEthernet1/1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,502,1002-1005
 switchport mode trunk
!
interface GigabitEthernet1/2
 ip address 6.0.0.254 255.255.255.0
!
interface GigabitEthernet5/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
```

```
 switchport mode trunk
 cdp enable
!
interface Vlan2
 ip address 192.168.1.1 255.255.255.0
 no mop enabled
 crypto map cm1
!
interface Vlan502
 no ip address
 crypto connect vlan 2
!
interface Tunnel1
 ip address 10.1.1.1 255.255.255.0
 tunnel source vlan2
 tunnel destination 192.168.1.254
!
ip route 5.0.0.0 255.255.255.0 Tunnel1
!
ip access-list extended acl1
 permit gre host 192.168.1.1 host 192.168.1.254
!
```

HSRP

For complete configuration information for HSRP, refer to this URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1833/products_feature_guide09186a0080086f3f.html

The reverse route injection (RRI) feature is used to allow dynamic routing information updates during the HSRP and IPSec failover. For complete configuration information on RRI support, refer to this URL:
http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_tech_note09186a00800942f7.shtml

HSRP has been coupled with IPSec to track state changes and provide a stateless IPSec failover mechanism. These sections provide HSRP configuration examples:

- Active Catalyst Switch Configuration, page 88
- Standby Catalyst Switch Configuration, page 90
- Remote Catalyst Switch Configuration, page 92

Note For guidelines on how to configure an IPSec stateful failover, see the "Using IPSec Stateful Failover and the VPN Module" section on page 36.

Active Catalyst Switch Configuration

The active Catalyst switch configuration is as follows:

```
Active# show run
Building configuration...

Current configuration : 2235 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Active
```

```
!
boot system flash sup-bootflash:
!
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
!
!
no ip domain-lookup
!
!
no mls ip multicast aggregate
no mls ip multicast non-rpf cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key NEEWOMM address 0.0.0.0 0.0.0.0
!
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
!
crypto map ha ha replay-interval inbound 10 outbound 1000
crypto map ha 10 ipsec-isakmp
 set peer 172.16.31.3
 set transform-set TS1
 match address 101
!
!
spanning-tree extend system-id
no spanning-tree vlan 4
!
!
!
interface GigabitEthernet1/1
 no ip address
 no ip redirects
 crypto connect vlan 4
!
interface GigabitEthernet1/2
 ip address 40.0.0.1 255.255.255.0
 no ip redirects
 standby delay minimum 35 reload 60
 standby ip 40.0.0.100
 standby timers 1 3
 standby preempt
 standby track GigabitEthernet1/1
!
interface GigabitEthernet3/1
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,4,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet3/2
 mtu 4500
```

```
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 ip address 172.16.31.1 255.255.255.0
 standby delay minimum 35 reload 60
 standby ip 172.16.31.100
 standby timers 1 3
 standby preempt
 standby name KNIGHTSOFNI
 standby track GigabitEthernet1/1
 standby track GigabitEthernet1/2
 crypto map ha redundancy KNIGHTSOFNI
!
ip classless
ip route 10.11.1.1 255.255.255.255 172.16.31.3
no ip http server
ip pim bidir-enable
!
access-list 101 permit ip host 40.0.0.3 host 10.11.1.1
arp 127.0.0.12 0000.2100.0000 ARPA
!
!
!
line con 0
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

Standby Catalyst Switch Configuration

The standby Catalyst switch configuration is as follows:

```
StandBy# show run
Building configuration...

Current configuration : 2236 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname StandBy
!
boot system flash sup-bootflash:
!
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
```

```
!
!
no ip domain-lookup
!
!
no mls ip multicast aggregate
no mls ip multicast non-rpf cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key NEEWOMM address 0.0.0.0 0.0.0.0
!
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
!
crypto map ha ha replay-interval inbound 10 outbound 1000
crypto map ha 10 ipsec-isakmp
 set peer 172.16.31.3
 set transform-set TS1
 match address 101
!
!
spanning-tree extend system-id
no spanning-tree vlan 4
!
!
!
interface GigabitEthernet1/1
 no ip address
 no ip redirects
 crypto connect vlan 4
!
interface GigabitEthernet1/2
 ip address 40.0.0.2 255.255.255.0
 no ip redirects
 standby delay minimum 35 reload 60
 standby ip 40.0.0.100
 standby timers 1 3
 standby preempt
 standby track GigabitEthernet1/1
!
interface GigabitEthernet3/1
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,4,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet3/2
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
```

```
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 ip address 172.16.31.2 255.255.255.0
 standby delay minimum 35 reload 60
 standby ip 172.16.31.100
 standby timers 1 3
 standby preempt
 standby name KNIGHTSOFNI
 standby track GigabitEthernet1/1
 standby track GigabitEthernet1/2
 crypto map ha redundancy KNIGHTSOFNI
!
ip classless
ip route 10.11.1.1 255.255.255.255 172.16.31.3
no ip http server
ip pim bidir-enable
!
access-list 101 permit ip host 40.0.0.3 host 10.11.1.1
arp 127.0.0.12 0000.2100.0000 ARPA
!
!
!
line con 0
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

Remote Catalyst Switch Configuration

The remote Catalyst switch configuration is as follows:

```
RemotePeer# show run
Building configuration...

Current configuration : 1674 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RemotePeer
!
boot system flash sup-bootflash:
!
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
!
!
no ip domain-lookup
!
no mls ip multicast aggregate
no mls ip multicast non-rpf cef
!
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key NEEWOMM address 0.0.0.0 0.0.0.0
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
!
crypto map ha 10 ipsec-isakmp
 set peer 172.16.31.100
 set transform-set TS1
 match address 101
!
spanning-tree extend system-id
!
!
!
interface Loopback1
 ip address 10.11.1.1 255.255.255.0
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 ip address 172.16.31.3 255.255.0.0
 crypto map ha
!
interface GigabitEthernet3/1
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet3/2
 mtu 4500
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 40.0.0.3 255.255.255.255 172.16.31.100
no ip http server
ip pim bidir-enable
!
access-list 101 permit ip host 10.11.1.1 host 40.0.0.3
arp 127.0.0.12 0000.2100.0000 ARPA
!
!
```

```
!
line con 0
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

QoS

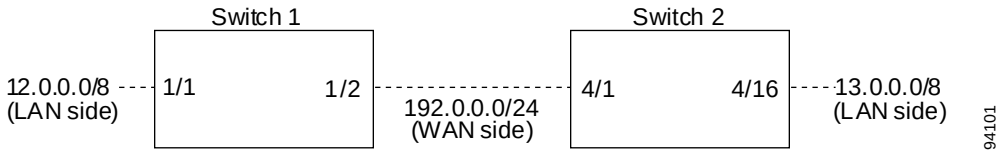
These sections provide configuration examples for QoS:

- Switch 1 Configuration, page 94
- Switch 2 Configuration, page 96

A summary of the switch configuration that is used in the examples is as follows (see Figure 16):

- The VPN module is in slot 3 on both switches.
- An IPSec tunnel that is between switch 1 and switch 2 encrypts all traffic.
- Both switches are configured so that IP packets with ToS 5 or ToS 7 go to high priority.
- To highlight the QoS configuration steps in the configuration examples, three exclamation points (!!!) precede each QoS-related command.

Figure 16 Configuring QoS Example



Switch 1 Configuration

The switch 1 configuration is as follows:

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch 1
!
boot system bootflash:c6k222-jk9sv-mz
logging snmp-authfail
!
ip subnet-zero
!
!
no ip domain-lookup
ip host tftp 223.255.254.254
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
```

```
!!! Enables qos globally
mls qos
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key 12345 address 192.0.0.2
!
!
crypto ipsec transform-set 3des_sha1_ts esp-3des esp-sha-hmac
!
crypto map cmap2 100 ipsec-isakmp
 set peer 192.0.0.2
 set transform-set 3des_sha1_ts
 match address acl0
!
!
spanning-tree extend system-id
no spanning-tree vlan 2
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
!
!
!
interface GigabitEthernet1/1
 ip address 12.0.0.1 255.0.0.0
 no keepalive
 speed nonegotiate
!!! Trust incomming ip precedence bits (from LAN side)
 mls qos trust ip-precedence
!
interface GigabitEthernet1/2
 no ip address
!!! Trust incomming ip precedence bits (from WAN side)
 mls qos trust ip-precedence
 crypto connect vlan 2
!
interface GigabitEthernet3/1
 no ip address
!!! COS 5 and 7 will go to high priority queue
 priority-queue cos-map 1 5 7
!!! Trust Ethernet frame COS bits
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet3/2
 no ip address
!!! This command is added automatically when /1 was configured
 priority-queue cos-map 1 5 7
!!! Trust Ethernet frame COS bits
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
!
interface Vlan2
 ip address 192.0.0.1 255.255.255.0
 no mop enabled
 crypto map cmap2
!
ip classless
ip route 13.0.0.0 255.0.0.0 192.0.0.2
no ip http server
no ip http secure-server
!
!
ip access-list extended acl0
 permit ip any any
!
!
!
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh acercon
!
end
```

Switch 2 Configuration

The switch 2 configuration is as follows:

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch 2
!
boot system bootflash:c6k222-jk9sv-mz
logging snmp-authfail
no logging console
!
ip subnet-zero
!
!
no ip domain-lookup
ip host tftp 223.255.254.254
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
!!! Enables qos globaly
mls qos
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key 12345 address 192.0.0.1
!
!
```

```
crypto ipsec transform-set 3des_sha1_ts esp-3des esp-sha-hmac
!
crypto map cmap2 100 ipsec-isakmp
 set peer 192.0.0.1
 set transform-set 3des_sha1_ts
 match address acl0
!
!
no spanning-tree vlan 2
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
!
!
interface GigabitEthernet3/1
 no ip address
!!! COS 5 and 7 will go to high priority queue
 priority-queue cos-map 1 5 7
!!! Trust Ethernet frame COS bits
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet3/2
 no ip address
!!! This command is added automatically when /1 was configured
 priority-queue cos-map 1 5 7
!!! Trust Ethernet frame COS bits
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
!
interface GigabitEthernet4/1
 no ip address
!!! Trust incomming ip precedence bits (from WAN side)
 mls qos trust ip-precedence
 crypto connect vlan 2
!
interface GigabitEthernet4/16
 ip address 13.0.0.1 255.0.0.0
!!! Trust incomming ip precedence bits (from LAN side)
 mls qos trust ip-precedence
!
interface Vlan2
 ip address 192.0.0.2 255.255.255.0
 no mop enabled
 crypto map cmap2
!
ip classless
ip route 12.0.0.0 255.0.0.0 192.0.0.1
```

```
no ip http server
no ip http secure-server
ip pim bidir-enable
!
!
ip access-list extended acl0
 permit ip any any
!
arp 127.0.0.12 0000.2100.0000 ARPA
!
!
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password a
 login
 transport input lat pad mop telnet rlogin udptn nasi ssh
!
end
```

Regulatory Standards Compliance

Catalyst 6500 series modules comply with the regulatory standards that are listed in the *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches* publication.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html